In the

United States Court of Appeals

For the Seventh Circuit

No. 20-3291

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ALEXANDER BEBRIS,

Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin.
No. 19-cr-2 — **William C. Griesbach**, *Judge*.

ARGUED MAY 13, 2021 — DECIDED JULY 15, 2021

Before SYKES, *Chief Judge*, and SCUDDER and KIRSCH, *Circuit Judges*.

KIRSCH, *Circuit Judge*. Alexander Bebris sent child pornography over Facebook's private user-to-user messaging system, Facebook Messenger, in 2018. Bebris's conduct was initially discovered and reported by Facebook, which licenses a "hashing" or (in overly simplified layman's terms) image-recognition technology developed by Microsoft called PhotoDNA. PhotoDNA provides the capability to scan

images uploaded onto a company's platform and compares the "hash" (or essence) of a photo with a database of known images of child pornography.[1] Thus, through that technology, three of Bebris's messages were flagged by PhotoDNA. Facebook employees reviewed the flagged images and reported them to the CyberTipline of the National Center for Missing and Exploited Children ("NCMEC"), as required by 18 U.S.C. § 2258A(a). NCMEC then reported the images to Wisconsin law enforcement officials, who eventually obtained a warrant and searched Bebris's residence, where they found a computer containing numerous child pornography files. Bebris was charged federally with possessing and distributing child pornography.

Bebris argued before the district court that the evidence against him should be suppressed, specifically contending that Facebook took on the role of a government agent (subject to Fourth Amendment requirements) by monitoring its platform for child pornography and reporting that content. On appeal, Bebris reprises this argument but primarily contends that he was deprived of the opportunity to prove that Facebook acted as a government agent because the district court denied his Federal Rule of Criminal Procedure 17(a) subpoena seeking pre-trial testimony from a Facebook employee with knowledge of Facebook's use of PhotoDNA. The district court, however, properly exercised its discretion in quashing

[1] The terms used in the record to describe the type of material in the database, which is administered by the National Center for Missing and Exploited Children, include "child exploitation material," "images depicting child sexual abuse," and "child pornography." The distinction between these terms, if any, is immaterial to the resolution of this appeal, and we will use the term child pornography in the interest of consistency.

that subpoena, as it sought cumulative testimony to material already in the record. The record included a written declaration from Microsoft and Facebook and live testimony from an executive at NCMEC, which administers the federal reporting system. On the merits, the district court did not err in its conclusion that Facebook did not act as a government agent in this case. Thus, we affirm.

I

Bebris sent messages to a woman via Facebook Messenger, a user-to-user private messaging service that is part of Facebook. PhotoDNA, a program developed by Microsoft and implemented in Facebook Messenger, flagged some of those messages, which contained images that matched known child pornography. PhotoDNA is an "image-mapping" technology that uses a mathematical algorithm to create a unique "hash value" based on the digital essence of a photo. The hash value of images uploaded and sent via Facebook Messenger are automatically compared to a database of the hash values of known child pornography, which is compiled and maintained by NCMEC. If the program returns a presumptive hit for child pornography, Facebook employees review the flagged images and then send the images and certain user information to NCMEC as "CyberTipline Reports," or "CyberTips," in accordance with 18 U.S.C. § 2258A.

In Bebris's case, three images were flagged as suspected child pornography and forwarded to NCMEC, which ultimately forwarded the information to state law enforcement agencies in Wisconsin. The Wisconsin authorities then subpoenaed internet data and identified the IP address that uploaded the photos as belonging to Bebris. They obtained a state search warrant and executed it at Bebris's residence,

where they seized numerous electronic devices, including a computer that contained numerous child pornography files.

Bebris was subsequently charged in federal court with possessing and distributing child pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B). He filed a motion to suppress evidence, arguing that Facebook (and NCMEC and law enforcement) violated his Fourth Amendment rights by searching his Facebook messages without a warrant. In support of that theory, Bebris argued that Facebook assumed the role of a government agent by monitoring for and reporting suspected child pornography to NCMEC. Bebris requested an evidentiary hearing and sought to elicit testimony relating to Facebook's cooperation with NCMEC and the government. Bebris additionally sought to elicit testimony from Facebook regarding whether he had an expectation of privacy over his Facebook messages and the scope of Facebook's search of his messages. Bebris argued in the alternative that even if Facebook did not act as a government agent, law enforcement impermissibly expanded Facebook's private search when it viewed images not previously opened by Facebook.[2]

The district court set the matter for an evidentiary hearing, and Bebris subpoenaed Microsoft, NCMEC, and Facebook, seeking testimony from each pursuant to Federal Rule of Criminal Procedure 17(a). Microsoft agreed to set forth certain facts in a stipulation. NCMEC agreed to make an executive available for the hearing.

---

[2] Bebris has not pressed this argument on appeal, and it is thus waived.

The Facebook subpoena, dated October 14, 2019, requested testimony from the "Person Most Knowledgeable of" three topics:

> (1) Facebook's use of PhotoDNA, "including but not limited to Facebook's agreement to sublicense the software, Facebook's policies and procedures in utilizing the software, information stored by Facebook which was discovered by use of the software, and Facebook's policies and procedures in reporting any content discovered by the software,"
>
> (2) "ongoing PhotoDNA training offered by Facebook and/or an outside entity," and
>
> (3) "cooperation" among Facebook, Microsoft, or NCMEC.

R. 41, Ex. 2. Following the receipt of the subpoena, Bebris's attorney and Facebook's attorneys attempted to agree on facts Facebook would stipulate to, but no agreement was reached. On November 27, 2019, Facebook filed a declaration from its Project Manager for Safety on the Community Operations team, Michael Francis Xavier Gillin, II. Facebook also filed a motion to quash the subpoena that same day, arguing that Gillin's declaration obviated the need for live testimony, which would be duplicative of those facts in the sworn declaration. At the December 3, 2019 evidentiary hearing, Facebook's attorneys appeared in the district court. The district court stated that it would set a briefing schedule for a response to the motion to quash and, in the event that Bebris prevailed on the motion, would continue the evidentiary hearing with Facebook's testimony at a later date. The

government stated that it viewed the declaration as sufficient for the court to rule on the motion to suppress without additional live testimony.

The evidentiary hearing proceeded with testimony from NCMEC Vice President John Shehan, who discussed (1) PhotoDNA and NCMEC's hash value database; (2) CyberTipline Reports; (3) oversight and funding of NCMEC by the United States government; and (4) NCMEC's partnership with Facebook. After the testimony concluded, the district court heard additional argument from Bebris, the government, and Facebook on the motion to quash. An attorney from Facebook stated that the company would be willing to supply a supplemental declaration addressing concerns raised by Bebris's counsel, specifically relating to the level of cooperation and training between NCMEC and Facebook and whether someone at Facebook had viewed the images before sending a report to NCMEC. In his supplemental brief, Bebris requested another evidentiary hearing and listed more than 100 questions he wanted to ask a Facebook witness at that hearing. In its supplemental response, Facebook argued that live testimony was not needed, and it provided a supplemental declaration from the same declarant, Gillin.

Gillin's declarations[3] stated, in relevant part, that:

(1) Facebook has an independent business purpose in keeping its platform safe and free from harmful content and conduct, including content that sexually

[3] Gillin's second declaration contained only minor changes from the first, clarifying the responses related to the training Facebook received from NCMEC and stating that a Facebook employee viewed flagged images before submitting them to NCMEC.

exploits children. As [its] Community Standards explain, "We do not allow content that sexually exploits or endangers children. When we become aware of apparent child exploitation, we report it to the National Center for Missing and Exploited Children (NCMEC), in compliance with applicable law." Our community Standards regarding Child Nudity and Sexual Exploitation of Children are publicly available on our website here: https://www.facebook.com/communitystandards/child_nudity_sexual_exploitation.

(2) Facebook identifies content and conduct that might violate its Community Standards in various ways. [The relevant CyberTipline Reports] were based on images Facebook identified using a software called PhotoDNA, which Facebook did not create but instead licensed directly from Microsoft, another private company. Facebook uses PhotoDNA software to identify potential child exploitation content, as well as to identify other types of violations of its Terms of Service or Community Standards. Information about how PhotoDNA works is publicly available, for example, at https://www.microsoft.com/en-us/photodna. Facebook did not license the software from NCMEC or anyone other than Microsoft directly.

(3) Facebook does not receive training from NCMEC regarding the use or operation of PhotoDNA or its processes for reporting to CyberTipline, meaning Facebook does not receive training from NCMEC on Facebook's own internal processes, including Facebook's use of PhotoDNA or Facebook's process of determining the content of its CyberTipline reports. NCMEC

may train or educate service providers, including Facebook, on the technical specifications and operation of the CyberTipline.

(4) [Paraphrased:] Gillin reviewed the reports created associated with this case. The photos instigating each report were viewed by a person at Facebook and sent to NCMEC.

(5) Although initially identified by PhotoDNA, a person viewed the images immediately before they were submitted to NCMEC. This is reflected in the CyberTipline Reports where the reports document "Did reporting ESP view the entire contents of uploaded files?" and the report reflects an answer of "Yes." When Facebook responds to this question with an affirmative "Yes," it means that a person viewed the image submitted in the CyberTipline report.

(6) Facebook has no record of receiving legal process from the Government for the account holders associated with the accounts reported in [the relevant CyberTipLine reports]. Prior to receipt of this subpoena, other than the initial submission of these two CyberTipline Reports, Facebook has identified no records of communication with NCMEC in this matter. Similarly, other than its counsel's communications with the Government about the defense subpoena, Facebook has identified no records of communications with the Government regarding the images or content of the CyberTipline reports.

R. 53, Ex. A.

Following supplemental briefing, the district court issued an order denying Bebris's motion to suppress and, within that order, granting Facebook's motion to quash. The district court found that Bebris lacked a reasonable expectation of privacy in his messages because Facebook's Community Standards and terms of service warned users that Facebook reports child pornography if it becomes aware that it is being sent. Separately, the district court held that Facebook searched Bebris's messages as a private actor and, thus, the search did not implicate the Fourth Amendment. Finally, the district court found that NCMEC and the Wisconsin law enforcement agencies did not exceed the scope of Facebook's private search.

Following that ruling, Bebris entered a guilty plea to one count of distributing child pornography, reserving his right to challenge the district court's denial of his motion to suppress on appeal. He was sentenced to 60 months in prison followed by six years of supervised release.

II

As a general, initial matter, Bebris's challenge to Facebook's search of his messages and his assertion that this search violated the Fourth Amendment draws from an argument that has become familiar to federal district and circuit courts around the country. Bebris's core theory is that Facebook's use of the PhotoDNA technology, along with other facts he presented or hoped to present (if they existed), converted Facebook into a government agent for Fourth Amendment purposes. Thus, Bebris contends that the evidence recovered and transferred as a result of Facebook's search should have been suppressed because it was obtained without a warrant. This theory is not novel and has been invoked in various circumstances involving PhotoDNA or similar

technology. See *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020); *United States v. Ringland*, 966 F.3d 731 (8th Cir. 2020); *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016); *United States v. Stevenson*, 727 F.3d 826 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012).

Bebris, however, has added a twist to this common argument. He asserts that he has been deprived of the opportunity to prove that Facebook acted as a government agent because the district court quashed his subpoena for live testimony from a Facebook representative at the evidentiary hearing on Bebris's motion to suppress. The district court's quashing of the subpoena, he argues, constituted a violation of the Confrontation Clause of the Sixth Amendment. In other words, Bebris argues that the ultimate denial of his motion to suppress (in which he claimed Fourth Amendment violations) was predicated on the district court's refusal to require testimony from a Facebook representative (which, as he sees it, violated his Sixth Amendment Confrontation Clause right). Bebris additionally argues that even if the district court did not err by quashing the Facebook subpoena, the district court still erred by denying the motion to suppress on the merits based on the evidence in the record. Bebris also argues that the district court erred by finding that he lacked a reasonable expectation of privacy in his Facebook messages. We address each argument in turn below.

A

1

Broadly, Bebris's arguments build from certain foundational assumptions, which we address at the outset. First,

recall that Facebook—which flagged and viewed the child pornography Bebris originally sent on its platform—sent a CyberTip to NCMEC, not directly to the Wisconsin authorities. Bebris hoped to prove that Facebook acted as an agent of NCMEC when Facebook searched and reviewed suspected child pornography, which, through an agency chain (law enforcement to NCMEC to Facebook), means that Facebook would be deemed a government agent. The government takes the position that NCMEC is not a government entity or agent, but calls this question immaterial. Because we hold below that the district court did not err in its determination that Facebook was a private actor in this case and the search was not later expanded, we agree that this question becomes immaterial. So, for purposes of this appeal, we assume that NCMEC is in fact a governmental entity or agent. See *Ackerman*, 831 F.3d at 1294–95 (discussing in depth whether NCMEC qualifies as a government entity or agent and concluding that it does). Thus, we proceed under the assumption that if Bebris could prove that Facebook acted as an agent of NCMEC, that agency relationship would serve as a basis for governmental action implicating the Fourth Amendment.

Second, Bebris assumes that the Sixth Amendment's Confrontation Clause is applicable during an evidentiary hearing on a motion to suppress. This assumption is not supported by the case law. "The opinions of [the Supreme Court] show that the right to confrontation is a *trial* right." *Pennsylvania v. Ritchie*, 480 U.S. 39, 52 (1987) (plurality opinion) (emphasis in original). This court and other circuit courts have endorsed the plain meaning of this *Ritchie* observation. See, *e.g.*, *United States v. Hamilton*, 107 F.3d 499, 503 (7th Cir. 1997) ("The Supreme Court has interpreted the [Confrontation Clause] to guarantee a defendant a face-to-face meeting with witnesses

appearing before the trier of fact.") (citation omitted); *Ebert v. Gaetz*, 610 F.3d 404, 414 (7th Cir. 2010) ("[B]ecause the court considered the statement at a suppression hearing, not Ebert's trial[,] the Confrontation Clause was not implicated.") (citing *United States v. Harris*, 403 U.S. 573, 584 (1971), which noted that the Confrontation Clause "seems inapposite to … proceedings under the Fourth Amendment"); *United States v. Thompson*, 533 F.3d 964, 969 (8th Cir. 2008) ("[T]he right of confrontation does not apply to the same extent at pretrial suppression hearings as it does at trial. [T]he interests at stake in a suppression hearing are of a lesser magnitude than those in the criminal trial itself.") (internal quotations and citations omitted).

To his credit, Bebris acknowledges in his briefing that "the Supreme Court has not yet clearly and decisively addressed whether the right to confrontation applies when a defendant has waged a challenge" related to the suppression of allegedly unconstitutionally obtained evidence. Appellant Br. 21. And Bebris makes substantial arguments for the extension of that right to an evidentiary hearing on a motion to suppress.[4] But we do not view our role as creating a new right where our own (and the most relevant Supreme Court) precedent suggests that no such right exists. With that in mind, we decline Bebris's invitation to review the district court's decision in quashing the Facebook subpoena under a Confrontation

[4] We agree with Bebris that the district court's reliance on *Linder v. United States*, 937 F.3d 1087 (7th Cir. 2019), appears to be misplaced, as that case dealt with somewhat novel and otherwise inapplicable circumstances. Bebris's other textual and precedential arguments, which rely on Supreme Court cases preceding *Ritchie*, are foreclosed in this case by the later developed Confrontation Clause doctrine.

Clause analysis—which would represent a novel holding that would have far-reaching and potentially unforeseen consequences for every suppression hearing. See *United States v. Marzook*, 435 F. Supp. 2d 708, 747–48 (N.D. Ill. 2006) (St. Eve, J.) (persuasively concluding that the Confrontation Clause does not apply to pre-trial suppression hearings and noting that Federal Rule of Evidence 104(a) provides that the rules of evidence do not bind a court making a determination at a suppression hearing, where hearsay and other evidence that would be inadmissible at trial may be relied on) (citing, inter alia, *United States v. Raddatz*, 447 U.S. 667, 679 (1980)).

The inapplicability of the Confrontation Clause to a suppression hearing does not mean, however, that a defendant seeking information to show that evidence was illegally obtained is left unprotected. Rather, district courts still must adhere to the traditional requirements that attach to their review of motions to suppress, including, as relevant here, in their discretionary determinations as to whether to issue or quash Rule 17 subpoenas. See FED. R. CRIM. P. 17.

2

Turning, then, to the district court's decision to quash Bebris's Rule 17(a) subpoena ad testificandum, we review that decision for abuse of discretion. *United States v. Hamdan*, 910 F.3d 351, 356 (7th Cir. 2018).[5] "We will reverse the district

[5] Although Rule 17(a), unlike Rule 17(c) (which governs subpoenas duces tecum), does not explicitly address the quashal or modification of a Rule 17(a) subpoena, courts "routinely have entertained motions seeking such relief and decided them by reference to comparable principles [to those governing Rule 17(c) subpoenas]." *Stern v. U.S. Dist. Court for Dist. of Mass.*, 214 F.3d 4, 17 (1st Cir. 2000).

court only 'when no reasonable person could take the view adopted by the trial court.'" *Id.* (quoting *United States v. Ozuna*, 561 F.3d 728, 738 (7th Cir. 2009)). Generally, Rule 17(a) subpoenas may issue where a defendant seeks testimony that is relevant and material to the issue being litigated. *Stern v. U.S. Dist. Ct. for Dist. of Mass.*, 214 F.3d 4, 17 (1st Cir. 2000). Where the sought testimony is cumulative or immaterial, a court does not abuse its discretion by quashing a Rule 17(a) subpoena. See *United States v. Beasley*, 479 F.2d 1124, 1128 (5th Cir. 1973). Moreover, Rule 17 may not be used to conduct a "fishing expedition." *United States v. Nixon*, 418 U.S. 683, 699–700 (1974) (analyzing Rule 17(c)).

As to the motion to suppress we review the district court's legal conclusions de novo and the district court's factual findings for clear error. *United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016). Mixed questions of law and fact are reviewed de novo. *United States v. Fiasche*, 520 F.3d 694, 697 (7th Cir. 2008). "We accord special deference to the district court's credibility determinations because the resolution of a motion to suppress is almost always a fact-specific inquiry, and it is the district court which heard the testimony and observed the witnesses at the suppression hearing." *United States v. Burnside*, 588 F.3d 511, 517 (7th Cir. 2009). To determine whether the district court abused its discretion in quashing the subpoena in this case, we must analyze the decision in the context of the underlying substantive legal argument that Bebris advanced in his motion to suppress.

The first clause of the Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated[.]" U.S. CONST. amend. IV. This

protection applies against governmental action and is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" *United States v. Jacobsen*, 466 U.S. 109, 113–14 (1984) (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). Where a private individual has discovered or been informed of a defendant's private information because the defendant has revealed it, that defendant's expectation of privacy in that information has been frustrated. *Id.* at 116–17. The controlling principle, distilled down, is that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed." *Id.* at 117 (internal quotations and citation omitted). Instead, "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* In other words, authorities typically may repeat a private search already conducted by a third party but may not expand on it—a legal principle that has been described as the private search doctrine. See *Ringland*, 966 F.3d at 736.

The government may not, however, simply enlist 'private' individuals to do its bidding in an attempt to avoid its Fourth Amendment obligations. An ostensibly private organization or individual may become a state actor for Fourth Amendment purposes in situations where the actor's conduct is "fairly attributable" to the government. *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295 (2001); see

United States v. Koenig, 856 F.2d 843, 849–50 (7th Cir. 1988). The defendant bears the burden of proving such a relationship. *United States v. Aldridge*, 642 F.3d 537, 541 (7th Cir. 2011). To meet this burden, "a defendant must prove some exercise of governmental power over the private entity, such that the private entity may be said to have acted on behalf of the government rather than for its own, private purposes." *Koenig*, 856 F.2d at 849. This determination must necessarily be made on a case-by-case basis, and no rigid formula has been articulated in this circuit, though two critical factors include (1) whether the government knew of and acquiesced in the intrusive conduct and (2) whether the private party's conduct was done with the purpose of assisting law enforcement or to further his own ends. *Id.* at 847 (citing *United States v. Feffer*, 831 F.2d 734, 739–40 (7th Cir. 1987)).

With this framework in mind, we return to the district court's decision to quash the Facebook subpoena, which Bebris claims deprived him of the ability to prove that Facebook acted as a government agent. In analyzing this issue, the district court determined that the record before it was sufficiently developed to conclude that Facebook was not a government actor. The district court further found that additional testimony by a Facebook executive was unnecessary. We agree.

First, as alluded to earlier, the district court was within its discretion to rely on the declarations submitted by Gillin because when determining preliminary questions about the admissibility of evidence, the district court is "not bound by evidence rules, except those on privilege." FED. R. EVID. 104(a); *United States v. Bolin*, 514 F.2d 554, 557 (7th Cir. 1975) ("[I]t is clear that hearsay evidence is admissible in a hearing on a

motion to suppress."). Second, the statements in the Gillin declarations, which were corroborated by NCMEC Vice President John Shehan's testimony, addressed the principal factual considerations relevant to the agency inquiry. Specifically, Gillin's declaration revealed that Facebook had not been directed by the government (or NCMEC) to take any specific action with respect to Bebris, that Facebook had not been in contact with the government or NCMEC with respect to Bebris prior to the discovery of child pornography in Bebris's messages, and that Facebook had its own independent business purpose in keeping its platform free of child pornography. On these first two points, Bebris argues that the district court erred by relying on the declaration "without any tested factual support" relating to whether the government compelled Facebook to perform this monitoring on its platform. In fact, however, NCMEC Vice President Shehan testified that Facebook's relationship with NCMEC was "completely voluntary." The district court's factual findings on this issue were not clearly erroneous, and additional testimony as to whether Facebook was compelled (in the face of the undisputed evidence properly before the court to the contrary) to monitor its platforms would have been cumulative.

As to Facebook's business purpose for monitoring its platform, Bebris argues that the district court erred by simply crediting Facebook's conclusory statement that it had an independent business purpose for monitoring its platform for child pornography. We disagree. True, Facebook's declaration stated that it had "an independent business purpose" for monitoring its platform for child pornography in a conclusory fashion. But the district court was entitled to determine, given the record before it, that this statement was sufficient. We note that the Microsoft stipulation, for example, states that "the

direct and indirect costs resulting from the presence of such images can be significant. For example, the presence of such images can increase the volume of consumer complaints received by Microsoft and, potentially, cause substantial harm to Microsoft's image and reputation in the marketplace." R. 43 at ¶ 4. Thus, the district court's finding as to Facebook's motivation, which was consistent with the common sense statement in the record provided by Microsoft, was proper. Several of our sister circuits have recognized that a company which automatically scans electronic communications on its platform does "not become a government agent merely because it had a mutual interest in eradicating child pornography from its platform." *Ringland*, 966 F.3d at 736. We agree—drawing from another well-stated opinion—that this sort of activity is analogous to shopkeepers that have sought to rid their physical spaces of criminal activity to protect their businesses. *Miller*, 982 F.3d at 425; see also *Stevenson*, 727 F.3d at 830 ("A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."); *Cameron*, 699 F.3d at 638 ("[I]t is certainly the case that combating child pornography is a government interest. However, this does not mean that Yahoo! cannot voluntarily choose to have the same interest.").

In the end, the district court appropriately relied on the Facebook declaration which, in conjunction with the NCMEC testimony, support its conclusion that Facebook was not acting as a government agent when it reviewed messages on its servers for child pornography and then reported that contraband to NCMEC. Because the sought-after live testimony as to the nature of the cooperation between Facebook and NCMEC would have been cumulative of Facebook's

declaration (which itself was corroborated by NCMEC testimony), the district court did not abuse its discretion in quashing the Facebook subpoena.

Turning to the merits of the motion to suppress, based on the evidence relied upon, which encompassed an appropriate universe of material, the district court's factual findings, including that Facebook did not act as government agent in this case, were proper. Bebris's additional arguments to the contrary are unavailing, including for the reasons discussed above. As a result, the district court properly denied Bebris's motion to suppress.

B

The parties have raised several additional arguments on appeal. Because we hold that the district court properly quashed the subpoena and denied the motion to suppress on the grounds discussed above, we need not reach whether Bebris had a reasonable expectation of privacy in his Facebook messages and whether the government actors in this case would benefit from the good-faith exception.

III

In sum, the district court did not err by quashing the subpoena to Facebook, and the district court did not err by denying the motion to suppress based on its finding that the private search doctrine applied.

AFFIRMED