NO.

IN THE
SUPREME COURT OF THE UNITED STATES

ALEXANDER P. BEBRIS,

Petitioner,

V.

UNITED STATES OF AMERICA,

Respondent.

PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

JASON D. LUCZAK
(*COUNSEL OF RECORD*)
GIMBEL, REILLY, GUERIN & BROWN LLP
TWO PLAZA EAST, SUITE 1170
330 EAST KILBOURN AVENUE
MILWAUKEE, WISCONSIN 53202
TELEPHONE: 414-271-1440

QUESTION PRESENTED FOR REVIEW

Does the Sixth Amendment and Confrontation Clause apply to all pretrial evidentiary hearings implicating the credibility of a witness?

LIST OF PARTIES

The parties to this action include the petitioner Alexander P. Bebris and the United States of America, the respondent. Facebook, Inc. intervened in the district court case by filing a motion to quash the subpoena and filed an amicus curiae brief at the United States Court of Appeals for the Seventh Circuit.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES

PAGE

CONSTITUTION, STATUTES AND RULES

OTHER AUTHORITIES

NO.

IN THE
SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 2021

ALEXANDER P. BEBRIS,

Petitioner,

V.

UNITED STATES OF AMERICA,

Respondent.

PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

Petitioner Alexander P. Bebris (Bebris) respectfully prays that a writ of certiorari be issued to review the decision of the United States Court of Appeals for the Seventh Circuit.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Seventh Circuit is reported at *United States v. Alexander P. Bebris*, 4 F.4th 551 (7th Cir. 2021). The decision of the United States District Court for the Eastern District of Wisconsin's decision to deny the defendant's motion to suppress evidence, and to grant Facebook, Inc.'s motion to quash is unreported and reprinted in the appendix. (A-37 to A-57).

JURISDICTIONAL GROUNDS

This petition arises from the Seventh Circuit's July 15, 2021, opinion affirming the district court's conviction of Bebris for possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B).

CONSTITUTIONAL AND STATUTORY PROVISIONS

The instant case involves the application of the Fourth, Fifth and Sixth Amendments of the U.S. Constitution and their interplay in a modern society where usage of social media programs and their messaging services has become a part of the daily lives of nearly all Americans.

The Fourth Amendment provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fifth Amendment provides as follows:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be

> subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.
>
> The Sixth Amendment provides as follows:
>
> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

STATEMENT OF THE CASE

On August 4, 2020, Mr. Bebris entered a conditional guilty plea to a single count of distribution of child pornography, contrary to 18 U.S.C. §2252A(a)(2)(A). (R.72). The parties agreed as part of the resolution that Mr. Bebris would retain the right

to appeal the district court's adverse rulings on his pretrial motion to suppress.

On November 17, 2010, the matter continued to sentencing, at which time Mr. Bebris was ordered to serve 60 months initial confinement, followed by six years of supervised release. (R.72;82).

Following his conviction and pursuant to the conditional plea, Mr. Bebris appealed his conviction to the Seventh Circuit. On appeal, he argued that the district court erred by denying his motion to suppress all evidence obtained from the illegal search of his private, user-to-user messages sent through the program Facebook Messenger. This search was conducted absent a warrant and in violation of the Fourth, Fifth and Sixth Amendments of the U.S. Constitution. Encompassed in his challenge of the district court's refusal to suppress was a secondary challenge to the district court's conclusion that as a

general matter, the Sixth Amendment does not apply to pretrial hearings, and the court's resulting order quashing the subpoena of Facebook, Inc., which denied Mr. Bebris the right to confront the corporation who conducted the search of his private messages. (R.86).

The Arrest and Charging of Alexander P. Bebris

On September 6, 2018, at 13:25:46 UTC, Facebook, Inc. (Facebook) submitted CyberTip 39932621 to the National Center of Missing and Exploited Children (NCMEC). (R.48:27). That CyberTip detailed that through the employment of Microsoft Corporation's PhotoDNA program, Facebook identified two images of suspected child pornography associated with the program user identified as "Alexander Bebris." (R.48:28). Three days later, Facebook submitted a second report to NCMEC, CyberTip 40017882, detailing one image of

suspected child pornography associated with Facebook user identified as "Alexander Paul." (*Id.*:40). According to both CyberTip reports, the images in question were sent through the Facebook Messenger user-to-user messaging platform and the intended recipient of both sets of images was a user identified as "Carly Macks." (*Id.*:27-40).

In December 2018, NCMEC submitted a referral containing the CyberTip reports to the Internet Crimes Against Children Task Force with the Wisconsin Department of Justice. (*Id.*:38). Investigators reviewed the information collected by and submitted from Facebook and NCMEC, including the images provided in the CyberTips, and provided this information to investigators at the Winnebago County Sheriff's Office. (R.30:2). On December 7, 2018, based on the information provided by NCMEC, investigators obtained an administrative subpoena to

obtain all account information related to Facebook usernames "Alexander Bebris", "Alexander Paul" and "Carly Macks." (*Id.*). Using the data received from the administrative subpoena, investigators determined the suspected users "Alexander Bebris" and "Alexander Paul" to be one in the same, and ultimately the defendant-appellant in this case, Alexander P. Bebris. (R.30:2-3).

On December 17, 2018, using the information obtained through Facebook's search and NCMEC's referral, investigators applied for a warrant to search Mr. Bebris' home and personal effects. (*Id.*). Police interviewed Mr. Bebris on scene and the search yielded several items of significance to the investigation, including a Dell computer that allegedly contained numerous files of interest to the government. (*Id.*). Bebris ultimately was arrested and indicted with one count of distribution of child

pornography and one count of possession of child pornography in Case No. 19-CR-02, contrary to sections 18 U.S.C. 2252A(a)(5)(B) and 18 U.S.C. 2252A(a)(2)(A). (*Id.*).

The Motion to Suppress & the Issuance of Subpoenas

On August 22, 2019, Bebris filed a motion to suppress all physical evidence and statements derived from the illegal search of his private user-to-user communications sent via Facebook Messenger, alleging that Facebook's actions were that of a government agent, and as a result, the Fourth Amendment mandated that a warrant be obtained before his private messages were searched and their contents seized.

At issue in the motion were three questions: (1) whether the National Center for Missing & Exploited Children (NCMEC) is a government entity or in the alternative, an agent of the government; (2) whether

Facebook, Inc. acted as an agent of the government or at the behest of the federal government; and (3) whether the search of Bebris's private user-to-user communications on Facebook Messenger constituted a Fourth Amendment search. (R.28;35). If the Fourth Amendment protected these messages, Bebris asserted that all evidence obtained as a result of the illegal search of his communications must be suppressed under the fruits of the poisonous tree doctrine pursuant to *Wong Sun v. U.S.*, 371 U.S. 471 (1963). (*Id.*).

Following receipt of the motion and upon the request of Bebris, the district court issued subpoenas for NCMEC, Facebook, Inc., and Microsoft, compelling their appearance and testimony at an evidentiary motion hearing as scheduled by the court. (R.34).

Microsoft's Response to the Subpoena

In mid-October 2019, Bebris served Microsoft Corporation, NCMEC, and Facebook, Inc. ("Facebook") with Federal Rule of Criminal Procedure 17 subpoenas issued by the district court. (R.40;41). Soon after, representatives from Microsoft contacted Bebris's counsel regarding a proposal to submit a written stipulation in lieu of providing live testimony. The parties, together with the corporation, agreed upon a set of facts set forth in a written stipulation to supplant live testimony of Microsoft at the evidentiary hearing. (R.49-1:¶4).

NCMEC's Response to the Subpoena

After receiving the district court subpoena, representatives from NCMEC advised that they intended to make an executive available for testimony. It was agreed upon that this would be done remotely via video. (R.46).

NCMEC agreed to participate in the hearing and was represented remotely by John Shehan, Vice President of the Exploited Child Division at NCMEC. During his testimony, Shehan focused primarily on four main topics: (1) the oversight and funding received by NCMEC from the federal government; (2) the organization's use of PhotoDNA and NCMEC's Hash-Value Database; (3) NCMEC's CyberTipline System; and (4) NCMEC's partnership with Facebook in its investigatory work. (R.48).

Shehan testified in detail about NCMEC's close relationship with Congress and the federal government. NCMEC, he asserted, receives approximately seventy-five percent of its funding from federal grants. (R.48:49:10-13). He acknowledged that at any time, Congress can pull its funding from NCMEC. (R.48:61:21-24). As a natural consequence of providing large amounts of funding to NCMEC,

Congress both monitors and oversees NCMEC's activities. (*Id.*)

For example, Mr. Shehan testified that in 2011, the Government Accountability Office (GAO) authored a report to Congress on NCMEC, which included the GAO conducting "a review of the operations." (R.48:58:15-20). In the report, it made various recommendations to NCMEC, including how to better assist law enforcement in initiating action, "such as obtaining a subpoena, initiating an investigation, or executing a search warrant." (R.48:61:2-8;Ex. C at 25). Additionally, in April 2016, the Department of Justice ("DOJ") wrote a report entitled "The National Strategy for Child Exploitation Prevention and Interdiction." (R.48:62:19-22;Ex. D). NCMEC participated in creating the report to the extent that they provided data related to the CyberTipline and the Child Victim Identification

Program. (R.48:63:5-24). This report summarizes NCMEC in the following way:

> The National Center for Missing & Exploited Children (NCMEC) is a private, non-profit organization *designated by Congress* to serve as the national clearinghouse on issues related to missing and exploited children and *works in cooperation with the DOJ and other federal, state, and local law enforcement*, education and social service agencies, families, and the public.

(R.48:Ex. D at 68)

The GAO report also detailed an initiative entitled the Child Victim Identification Program, which helps NCMEC "track child pornography images of children previously identified by law enforcement." (*Id.* at 69). The report goes on to state that the program's "mission is to assist federal and state law enforcement agencies in their efforts to identify, located and rescues child victims in sexually exploitive situations." (*Id.*).

Beyond the funding and oversight of NCMEC, Mr. Shehan asserted that Congress has given NCMEC power and responsibility under federal law; powers that only law enforcement have. (R.48:49:5-7); see also, *e.g.*, 42 U.S.C. §5773(b). Congress has authorized NCMEC by federal statute to participate in activities which ordinary citizens may not. (R.48:48:22-49:2). For instance, NCMEC is allowed by law to both possess and distribute child pornography. (R.48:49:14-18); see also 18 U.S.C. §2258A(g)(3), 18 U.S.C. §2258C(a). Additionally, Congress has delineated numerous duties and responsibilities of NCMEC, such as NCMEC's responsibility to forward the CyberTipline Reports to law enforcement agencies. (R.48:49:19-23); see also 18 U.S.C. §2258A(c), (g)(3).

Shehan testified that the software program, PhotoDNA, was developed by Microsoft in conjunction

with Dartmouth College. The software creates an independent hash value for each digital image analyzed with the program. (R.48:17:7-9; 20:1-8; R.43:¶3). A hash value is a unique identifier for a digital image. (R.43:¶¶6-7). NCMEC and various Electronic Service Providers (ESPs) use PhotoDNA to identify potential images of child pornography and deliver the contraband to the government. (R.48:20:1-8; R.43:¶8).

From the development of PhotoDNA up until approximately three years ago, Microsoft allowed NCMEC to sublicense the program to any entity for free, a process that permitted NCMEC to provide ESPs like Facebook the program without any cost to the provider. (R.48:17:22-18:12). Microsoft has now given its sublicense authority over to a different

group, the Technology Coalition[1], an organization whose members are various ESPs, including Facebook and Microsoft. (R.48:47:10-12, 22-25).

Mr. Shehan continued, explain that NCMEC, as authorized by Congress, stores all hash values of suspected or known contraband in its automated Hash Value Database[2], the nation's clearinghouse of child pornography. (R.48:21:1-3; 67:10-12). This

---

[1] While NCMEC is not a "member" of the Technology Coalition, the two entities are not mutually exclusive. The Technology Coalition hosts an annual conference which NCMEC attends and in which it is an active participant. (R.48:70:17-21). NCMEC also collaborates with the Technology Coalition, as it updates the group on its own investigative activities and use of the PhotoDNA software, including trends and the CyberTipline. (*Id.*:48:3-9). Mr. Shehan testified that NCMEC "certainly" partners and collaborates with the Technology Coalition whenever it can. (*Id.*:48:14-16).

[2] Mr. Shehan testified that about fifty companies, including Facebook, have access to NCMEC's hash sharing platform (*Id.*:23:2-3), but that a handful of private databases also exist (*Id.*:73:23-25). He stated that NCMEC has no way of knowing whether CyberTipline Reports from ESPs are based on images found using NCMEC's hash sharing platform or a separate private database. (*Id.*:74:1-4). What program was used to identify the suspected images in this case by Facebook is a fact that is unknown to NCMEC, one that only a representative of Facebook could properly attest to.

database contains "every single file from every report [NCMEC] ever received." (R.48:21:10-12). Since its inception, NCMEC has received over sixty million CyberTipline[3] reports. (R.48:38:6).

Shehan also testified that to more effectively investigate potential possession of contraband, NCMEC provides ESPs with access to its Hash Value Database. (R.48:21:21-23). Not only can ESPs access the database and share hash values amongst themselves, NCMEC proactively provides ESPs the hash value or image fingerprint of those images it finds "egregious" and thus are of particular interest to it and law enforcement. (*Id.*:21:13-16). This is done so that a more targeted, specific search of ESP user data can be conducted. (*Id.*).

---

[3] Since its implementation in 1998, NCMEC's CyberTipline, has grown exponentially. (*Id.*:15:19-16:23). In 2018 alone, NCMEC had received and processed over eighteen million CyberTipline Reports. (*Id.*:16:22-23).

Mr. Shehan explain that after alleged contraband is identified by an ESP, federal law requires it be reported to NCMEC through its CyberTipline reporting system, as set forth in 18 U.S.C. §2258B(a). Once a CyberTip is received from an ESP, NCMEC makes its own independent determination of whether the images are child pornography and thus, its possession prohibited. *Id.* Following that determination, NCMEC determines to which law enforcement agency the report must be sent. (R.48:29:15, 35:20-38:17, 66:7-19).

Shehan testified that a CyberTipline report consists of four sections, labeled A through D. (*Id.*:29:13-15; see also R.48:Ex.A, B). Section A is filled out by the reporting ESP, and there, an ESP must disclose the name/identity of the tip submitter and how the point of contact can be reached by law enforcement for follow up; the incident type and time

it was identified; the URL; known information on the user being reported; any additional information the ESP would like to include and information regarding the uploaded suspected contraband. (R.48:Ex.A).

Section A also asks: "Did the Reporting ESP view the entire contents of the uploaded file?" In both CyberTipline Reports associated with this case, Facebook answered "yes." (*Id.*:Ex.A, B.). Of significant importance to the issue here, Mr. Shehan testified that answering "yes" to this inquiry does not mean that the ESP viewed the image at the time the report was created, leaving for the possibility that it was viewed sometime later and at the behest of another person or body. (*Id.*:46:11-13). Mr. Shehan also testified to the importance of ESPs responding "yes" to the question:

> [ATTY. PROCTOR] . . . you mentioned if the answer

> provided by the provider is "no," the NCMEC could not look at the file that was uploaded as part of the CyberTipline; is that correct?
>
> [SHEHAN] A. Correct. There's actually a lock icon that goes over the file. It cannot be viewed by the [NCMEC] staff member. And the same applies if they do not answer. So if they do not say "yes" and gets "information not provided," it's also locked and the staff member cannot view that file.
>
> Q. Why is it locked?
>
> A. Well, it was after a few previous court cases that we felt it was prudent to provide better clarity into these reports as to who is viewing, who is not viewing, and also respect what some of those decisions had been in regards to what files the NCMEC could and should not view."

(*Id.*:33:8-22).

Mr. Shehan asserted that once NCMEC receives a tip, it reviews the report and decides whether to send the report to a law enforcement

agency. (*Id.*:66:13-16). If NCMEC turns over the report to a law enforcement agency, it does so through a virtual private network ("VPN"). (*Id.*:50:2-7; 57:20-25). The agency can then log in through a VPN to view the CyberTipline Reports. (R.48:57:14-19; 50:2-7; 57:20-25). Because of the large volume of CyberTipline Reports passed on to various law enforcement agencies, NCMEC sends each agency a daily summary of all the reports within the agency's jurisdiction, making it easier for the law enforcement agency to track their submissions for the purposes of investigating the alleged offender, demonstrating how NCMEC and law enforcement work together to further these prosecutions. (R.48:57:14-19).

Facebook's Response to the Subpoena

In contrast to Microsoft and NCMEC's response to the subpoenas, Facebook neither agreed to testify, nor did it engage with counsel to develop a stipulated

set of facts that could be submitted for the court's review in lieu of live testimony.

Instead, representatives of Facebook did not contact Bebris's counsel until shortly before the hearing, and at that time, they requested permission from Bebris to submit a declaration of its position in lieu of live testimony and confrontation. (R.49-1:¶4). Defense counsel, in an effort to accommodate the company and preserve its resources, notified Facebook that it would accept a declaration in lieu of its appearance, but only if such a declaration answered all questions Bebris believed to be relevant and necessary to a full and proper determination of the merits of the motion. (*Id.*:¶¶4, 5, Ex. A). To assist in facilitating Facebook's request, Bebris promptly provided a list of topics and questions relevant to the motion that it sought answered in any declaration if

it were to take the place of live testimony and confrontation. (*Id.*).

On November 27, 2019, less than a week before the hearing, Facebook submitted a two-and-a-half-page declaration that largely ignored the topics presented and questions asked by Mr. Bebris. (R.41). Accompanying the declaration was a motion from Facebook requesting to quash the court ordered subpoena, asserting that the subpoena was unreasonable and oppressive, and that its testimony was not relevant or necessary to the issues at hand. (R.40).

The newly filed declaration and motion to quash was addressed at the outset of the December 3, 2019 evidentiary hearing. (R.48:4-8). The court and parties agreed to set Facebook's motion for briefing with the understanding that the evidentiary portion of the motion hearing would remain open until the

court decided whether the corporation could be compelled by Bebris to testify. (R.48:6).

The declaration submitted by Facebook contained very little information and some claims that were directly undermined by the testimony of John Shehan. For example, despite Facebook's declaration that claimed no partnership existed or currently exists between Facebook and NCMEC, Mr. Shehan's testimony painted a very different picture. (R.41). He described a hand-in-hand working relationship, including trainings, support, and additional projects. (R.48:42-43).

Further, Facebook explicitly declared that the corporation "does not receive training from NCMEC regarding the use or operation of the PhotoDNA software or its processes for reporting to the CyberTipline." (R.41:¶4). However, Shehan testified

NCMEC provides training[4] on the CyberTipline to all reporting ESPs, including Facebook. (R.48:25:1-5)

Shehan estimated that NCMEC communicates with Facebook regarding the CyberTipline "at least monthly." (R.48:42:4-6). He stressed that he "would think that [NCMEC] do[es] spend quite a bit of time educating [Facebook] on reporting into the CyberTipline." (*Id.*:45:1-3). His testimony also shed light on formal trainings NCMEC provides to Facebook, with the most recent being just six months prior to his testimony. (*Id.*:43:1-7). For this training, NCMEC traveled directly to Facebook's facilities to educate the company's employees. (*Id.*).

Not only does NCMEC provide numerous trainings to Facebook, but Facebook provides both in-

[4] "Sure. We certainly provide training. Especially when a company first begins to report into the CyberTipline, we want to make sure they understand what the fields are, what it is that they think that they are reporting actually came through in the submission process." (R.48:25:1-5).

kind and financial support to NCMEC. (*Id.*:24:5-8) Mr. Shehan testified that Facebook "provide[s] in-kind and financial support to the [NCMEC] as well. So in many ways they are, you know, a partner to our organization and they help us to better fulfill our mission." (*Id.*).

Finally, Mr. Shehan testified that the relationship between NCMEC and Facebook is so close that they are in the process of developing a new project together related to the Amber Alert Program and how to best disseminate information on missing children through Facebook's numerous platforms. (*Id.*:23:18-24:4).

As a result of Mr. Shehan's detailed testimony, it became clear to Mr. Bebris that Facebook's written declaration was lacking and inconsistent with the facts elicited at the evidentiary hearing and

insufficient to stand in the place of live testimony and confrontation.

The Written Decision Denying Suppression

a. The District Court Quashes Facebook's Subpoena

As a general matter, the district court held that the Sixth Amendment right to compulsory process is "a trial right" and "does not apply to pretrial proceedings," citing *Linder v. U.S.,* 937 F.3d 1087, 1090 (7th Cir. 2019). (R.60:7). The district court continued and found that the testimony of Facebook was not needed to determine the level of cooperation between NCMEC, the federal government and Facebook because as a general matter, such cooperation "would not transform Facebook into a government agent or instrumentality." (R.60:5-8).

b. The District Court Holds that Mr. Bebris Has No Privacy Interest in his Facebook Messages

Citing *U.S. v. Villegas,* 495 F.3d 761 (7th Cir. 2007), the district court held that when determining whether one has a privacy interest protected by the Fourth Amendment, it must consider whether the individual had "an actual subjective expectation of privacy and that the expectation is one that society is prepared to recognize." (R.60:2; App.109). In its analysis, the court looked to Facebook's declaration and its reference to its "Community Standards" policy available publicly on a section of its website. (*Id.*:3; App.110).

The court wrote, "Facebook has a corporate policy that prohibits content that sexually exploits or endangers children" and that when Facebook "become[s] aware of apparent child exploitation," the exploitation is reported to NCMEC as required by

applicable law. (*Id.*). "In the face of these disclosures," the court wrote, "any expectation of privacy Bebris had with respect to child pornography uploaded via his Facebook Messenger account would be objectively unreasonable." (*Id.*).

Alternatively, the district court concluded that even if Bebris had an objectively reasonable expectation of privacy in his user-to-user Facebook Messenger communications, "because Facebook is not a government agent," the Fourth Amendment is not implicated, and the search was a private one permitted under the law. (R.60:5-6; App.112-13). The court found that "the government neither knew or nor acquiesced in Facebook's monitoring of Bebris' emails." (R.60:6; App.113). Relying upon the declaration, the court accepted that Facebook monitored the content of its users' private messages because "[n]o sane person, let alone a business that

values its image and reputation, wants to be publicly associated with the sexual exploitation of children." (*Id.*).

c. The District Court Holds that Facebook is not an Agent of the Government

The court held that even if NCMEC is a government entity or acting as an agent of the government, the court relied upon the company's declaration and opined that Facebook's search was a private one and was not expanded upon by NCMEC, as an individual had viewed the photograph before the CyberTipline was sent. (R.60:8; App.115).

And, even if the company had not viewed the image prior to submitting the report, the court found that the use of the hash value program, PhotoDNA, is so specific that a subsequent viewing of the image by the government or its actors absent consent or a warrant is not a "significant expansion of a search

previously conducted by a private party such that it would constitute a separate search." (*Id.*:9; App.116).

Appeal to the Seventh Circuit

Mr. Bebris appealed the adverse decision of the district court to the Seventh Circuit of the U.S. Court of Appeals. The appellate court considered each of Bebris's arguments and ultimately affirmed the decision of the lower court denying suppression. (R.97).

Before engaging in its analysis of the specific facts presented by Bebris's case, the Seventh Circuit discussed two legal concepts that underly the questions before it as posed by Mr. Bebris.

First, the Seventh Circuit discussed the premise that NCMEC is a government entity. The reviewing court accepted this concept for the sake of this appeal, relying upon *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). (R.97:11). Therefore,

for the purposes of review, the court operated under the concept that if Mr. Bebris could establish that Facebook, Inc. was operating as an agent of NCMEC when it searched Bebris's private user-to-user messages, it "would serve as a basis for government action implicating the Fourth Amendment." (*Id.*).

Next, the appellate court held that contrary to Mr. Bebris's position, case law coming out of the U.S. Supreme Court, *i.e. Pennsylvania v. Ritchie*, 480 W.S. 39, 52 (1987) (plurality opinion), did not support the contention that the Sixth Amendment's Confrontation Clause applied to pretrial litigation. (*Id.*). The Seventh Circuit agreed that while "'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," it declined the invitation to create such a

right without such guidance from the Supreme Court. (*Id.*:12). The court of appeals opined that even though confrontation is not a right that exists pretrial, a defendant may still compel the testimony of a necessary witness, but pursuant to the discretion of the circuit court. (*Id.*:13).

Regarding the merits of the motion, the appellate court found that the district court did not abuse its discretion in quashing the subpoena compelling Facebook, Inc. to provide testimony regarding its activities. (*Id.*:16-17). First, the court held that the pretrial proceeding implicated by Mr. Bebris's motion to suppress was not bound by the rules of evidence and therefore, the court need not honor the subpoena request from the outset. (*Id.*:16-17).

Second, the court found that the areas of testimony relevant to Mr. Bebris's contention that

there was significant cooperation between NCMEC and Facebook and that Facebook's cooperation with NCMEC and government prosecutions was compulsory were largely addressed by the testimony of John Shehan. (*Id.*). Therefore, the court held, additional testimony would have been cumulative. (*Id.*:17).

Third, regarding the company's purpose and objectives in monitoring the messages of its users like it did in this case, the court of appeal disagreed with Mr. Bebris's claim that Facebook's brief blanket assertion that it had "an independent business purpose" was insufficient. (*Id.*). The court of appeals pointed to holdings in other circuits that arrived at similar conclusions – that performing automatic scans of electronic communication platforms does not make a corporation "a government agent merely because it had a mutual interest in eradicating child

pornography from its platform." (*Id.*:18, citing *United States v. Ringland*, 966 F.3d 731 (8th Cir. 2020)). That the district court arrived at the same conclusion was not an abuse of discretion. (*Id.*).

Applying these conclusions to the facts and issues presented here, the Seventh Circuit held that based upon those findings and the record presented on appeal, "the district court's factual findings, including that Facebook did not act as government agent in this case, were proper." (*Id.*:19). Therefore, the district court's denial of the motion to suppress on this basis was likewise proper[5]. (*Id.*).

---

[5] Because the Seventh Circuit resolved the issue on this basis, it did not reach additional questions posed by this factual scenario and in the appellate briefs (such as whether Bebris had a reasonable expectation of privacy in his Facebook messages and whether the good-faith exception would be applicable if the court were to find that Facebook is indeed a government agent). (*Id.*:19)

REASONS FOR GRANTING THE WRIT

While the underlying factual scenario, relationships involved and internet-based systems implicated in this appeal present a uniquely complicated and modern set of circumstances, the question posed by this petition is simple – does the Sixth Amendment Confrontation Clause have any place in pretrial criminal litigation or has the age-old foundational constitutional principle been relegated to the sidelines by procedural rules meant to increase efficiency in our federal courts?

Here, Mr. Bebris, a citizen of the United States of America, contends that Facebook, Inc., in all its power and reach, conducted an illegal and extensive search of his private user-to-user messages as part of its admittedly regular monitoring of its userbase's private activities. Facebook, Inc., with the assistance of the district court, has been able to dodge the

question of why the company reviews its user's messages, the purpose of doing so and how the company goes about this process.

In Mr. Bebris's case, Facebook may not draw the ire of the public because the allegation is of course that he violated the law in his use of the private user-to-user messaging platform. But this process of reviewing private messages of users most definitely does not begin and end with Mr. Bebris, and the company's practice of systematically invading its user's privacy is one that is seemingly being carried out at the direction of the federal government.

Citing the language of this body in *Pennsylvania v. Ritchie*, 480 W.S. 39, 52 (1987) (a holding without majority agreement), the Seventh Circuit and its counterparts throughout the country have been denying individuals the ability to confront entities – corporations, non-profits, and law

enforcement – who are invading citizen's private spaces and reviewing their personal correspondence on the premise that the right to confront one's accuser is reserved only for a trial.

The Sixth Amendment to the United States Constitution reads:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

U.S. Const. VI Amendment. Those words, "in all criminal prosecutions," signify that the right to confrontation is one that applies to all constitutionally afforded proceedings involved in a criminal prosecution. While this court has never made this the

law in a clear and decisive majority, its holdings in other matters involving confrontation indicate that the lower courts have got it wrong.

This court's decision in *Crawford v. Washington*, 541 U.S. 36 (2004), and its accompanying concurrence, set forth a detailed historical assessment of the confrontation clause and its importance in criminal jurisprudence. The opinion concludes that "[w]here testimonial statements are at issue, the only indicium of reliability sufficient to satisfy constitutional demands is the one of the Constitution actually prescribes: confrontation." *Crawford*, 541 U.S. at 68-69. The *Crawford* Court continued, holding that "[d]ispensing with confrontation because testimony is *obviously* reliable is akin to dispensing with jury trial because a defendant is *obviously* guilty. This is not what the

sixth Amendment prescribes." *Id.* at 62 (emphasis added).

Even decades before *Crawford* and *Ritchie*, this Court plainly assumed the Confrontation Clause applied to a pretrial suppression hearing in *McCray v. Illinois,* 386 U.S. 300, 305 (1967). There, the Court was considering whether a defendant could compel the identity of an informant through the cross-examination of a witness at a suppression hearing. The Court held that the trial court's refusal to permit the line of questioning was not a violation of the Confrontation Clause, *specifically not because the Clause did not apply at a suppression hearing*, but because it was not relevant to the question of suppression based on the facts and circumstances of the case and also because well-settled Illinois law permitted police to withhold the identity of an

informant when the issue of guilt or innocence was not implicated. *McCray*, 386 U.S. at 305.

Further, the lower courts' misplaced reliance on *Ritchie* ignores that suppression issues may be dealt with in the midst of trial and therefore, Confrontation would apply. If the right to confrontation applies during such an inquiry at trial, but not at a nearly identical pretrial hearing, is there not a denial of due process for some but not others based only on the procedural progression of his or her case?

Historically, a review of the applicable case law[6] suggests that the suppression of

---

[6] *See, e.g., Gannett Co, Inc. v. DePasquale*, 443 U.S. 368, 437 (1979) (Blackmun, J., concurring in part and dissenting in part) ("Indeed, the modern suppression hearing, unknown at common law, is a type of objection to evidence such as took place at common law…in open court…");

See, e.g., Gannett Co, Inc., 443 U.S. at 395-96 (Burger, C.J., concurring). "When the Sixth Amendment was written, and for more than a century after that, no one could have conceived that the exclusionary rule and pretrial motions to suppress evidence would be part of our criminal jurisprudence."

unconstitutionally obtained evidence historically occurred amid the trial on the merits. It was only after the passage of time and the crescendo of case volume that practice of addressing suppression at trial has become less common as courts favor pretrial litigation of evidentiary issues rather than interrupting the trial and delaying an already empaneled jury. The practice of addressing suppression matters pretrial

---

See, e.g. 3 Wayne R. LaFave, CRIMINAL PROCEDURE §10.1(a) (4th ed. 2016) ("At one time, it was not uncommon for states to treat objections to illegally obtained evidence as subject to the usual principle that the admissibility of evidence is determined when it is tendered and not in advance of trial. A few jurisdictions still follow [this approach]…") (internal quotation marks omitted).

See, e.g., U.S. v. Nixon, 418 U.S. 683, 702, 94 S. Ct. 3090, 3104 (1974) ("Enforcement of a ***pretrial subpoena*** duces tecum must necessarily be committed to the sound discretion of the trial court since the necessity for the subpoena most often turns upon a determination of factual issues. Without a determination of arbitrariness or that the trial court finding was without record support, an appellate court will not ordinarily disturb a finding that the applicant for a subpoena complied with Rule 17(c).") (internal quotation marks omitted) (emphasis added).

has now been codified in the Federal Rules of Procedure, which states:

> In the interest of normal procedural orderliness, a motion to suppress, under Rule 41(e), must be made prior to trial, if the defendant then has knowledge of the grounds on which to base the motion…This provision…requiring the motion to suppress to be made before trial, is a crystallization of decisions of this Court requiring that procedure, and is designed to eliminate from the trial disputes over police conduct not immediately relevant to the question of guilt.

Jones v. U.S., 362 U.S. 257, 264 (1960), *overruled on other grounds*, *U.S. v. Salvucci*, 448 U.S. 83 (1980).

That the timeline of a suppression hearing has changed over the years does not alter the rights effected by the matter, as "[a] rule of practice must not be allowed for any technical reason to prevail over a constitutional right." *Gouled v. U.S.*, 255 U.S. 298, 313 (1921), *abrogated on other grounds Warden Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967). This

same line of thinking was employed in the holding concluding that the Sixth Amendment public-trial right applied to suppression hearings – that a "temporal factor" does not control the constitutional analysis. *Gannett Co, Inc. v. DePasquale*, 443 U.S. 368, 436-37 (1979) (Blackmun, J., concurring in part and dissenting in part).

Acceptance of this case will allow this Court to provide necessary guidance with a holding that makes it clear – the Confrontation Clause applies to all criminal evidentiary hearings when credibility of a relevant witness is at issue. Certainly, the Framers of the U.S. Constitution and our founding fathers did not intend for a modern rule of criminal procedure to strip away a defendant's ability to confront witnesses who can speak to the legality of a search of their private effects and personal communications, particularly when those witnesses are aligned with

the government or other dominating and powerful forces operating in our nation. To give the judiciary the power to act as the arbiter of truth in matters of such importance without first requiring the court to witness the testimony firsthand would be to undermine one of the hallmarks of our adversarial system.

If this court were to hold that the Confrontation Clause does not apply to pretrial criminal proceedings, the impact of such a landmark ruling would be destructive to our criminal justice system at such a substantial level, it is difficult to put into words. Law enforcement and its agents would be able to interfere with the lives and monitor the daily activities of individuals throughout our nation with impunity and our citizenry denied any true venue or procedure for recompense.

That the holdings in this case imply that reliance upon the uncontested word of Facebook, Inc. and other monoliths like it is an acceptable substitute for live testimony and confrontation so long as the trial court does not abuse its discretion in doing so sets the stage for these massive corporate entities and their government counterparts to take advantage of the veil of secrecy that has been bestowed upon them.

As the recent hearings held by our Congress have shown, Facebook, Inc. is not the altruistic actor, waging war against those who take advantage of children, they held themselves out to be in the declaration entered in this case. It appears, they are in fact quite the opposite. Just last week, Facebook whistleblower Frances Haugen said[7] during her

[7] Protecting Kids Online: Testimony from a Facebook Whistleblower, October 5, 2021,

October 5, 2021 testimony to the U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Data Security: "It is clear that Facebook prioritizes profit over the well-being of children and all users." And now, with courts throughout the nation siding with Facebook, Inc. and the like and finding that they need not be subjected to confrontation on questions such as this, individuals are down one more tool in the seemingly never-ending fight for privacy in their communications.

It is for those reasons that Mr. Bebris implores this court to accept review of his case and to conclude that the confrontation clause applies to all pretrial

---

https://www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower, accessed October 11, 2021; Here are 4 key points from the Facebook whistleblower's testimony on Capitol Hill, National Public Radio, October 5, 2021, https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress, accessed October 11, 2021.

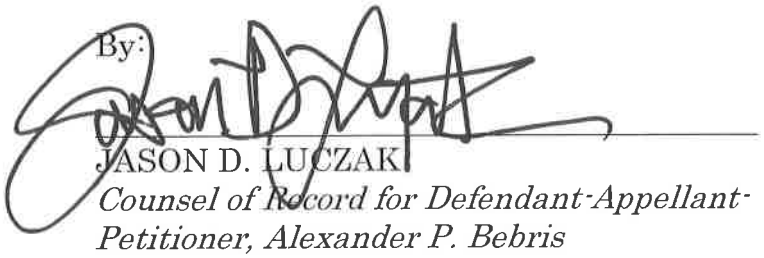
criminal evidentiary proceedings where a witness's credibility is at issue.

Dated this 12th day of October, 2021.

Respectfully submitted,

GIMBEL, REILLY, GUERIN & BROWN LLP

By:



JASON D. LUCZAK
Counsel of Record for Defendant-Appellant-Petitioner, Alexander P. Bebris

POST OFFICE ADDRESS:

Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440

NO.

IN THE
SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 2021

ALEXANDER P. BEBRIS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

APPENDIX TO PETITION FOR WRIT OF CERTIORARI

JASON D. LUCZAK
(*COUNSEL OF RECORD*)
GIMBEL, REILLY, GUERIN & BROWN LLP
TWO PLAZA EAST, SUITE 1170
330 EAST KILBOURN AVENUE
MILWAUKEE, WISCONSIN 53202
TELEPHONE: 414-271-1440

TABLE OF CONTENTS OF APPENDIX

In the
United States Court of Appeals
For the Seventh Circuit
UNITED STATES of America, Plaintiff–Appellee,
v.
Alexander BEBRIS, Defendant–Appellant.

No. 20-3291.
Argued May 13 ,2021.
Decided July 15, 2021.

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

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.

---

[1] The terms used in the record to describe the type of material in the data- base, 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.

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 Face- book acted as a government agent because the district court denied his Federal Rule of Criminal Procedure 17(a) subpoena seeking pretrial testimony from a Facebook employee with knowledge of Facebook's use of PhotoDNA. The district court, however, properly exercised its discretion in quashing 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 in- formation 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 up- loaded 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 ipermissibly 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.

The Facebook subpoena, dated October 14, 2019, re- quested 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

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

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 Face- book. 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 some- one at Facebook had viewed the images before sending a re- port 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 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.

---

[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 be- fore submitting them to NCMEC.

(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 Face- book 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 as- sociated with this case. The photos instigating each re- port 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 sub- mitted 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 im- age 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 im- plicate 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 sup- press 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 Face- book'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 Face- book'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 re- covered and transferred as a result of Facebook's search should have been suppressed because it was obtained with- out 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 sup- press (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 Face- book 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 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.*

[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.

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 ad- here 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 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*

[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).

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 con- duct 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 Face- book 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 plat- form, Bebris argues that the district court erred by simply crediting Facebook's conclusory statement that it had an in- dependent 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

United States District Court
Eastern District of Wisconsin
UNITED STATES of America, Plaintiff–Appellee,
v.
Alexander BEBRIS, Defendant–Appellant.

Case No. 19-CR-02.

Ordered March 9, 2020.

DECISION AND ORDER DENYING MOTION TO SUPPRESS

On January 15, 2019, a grand jury sitting in Milwaukee returned an Indictment charging Defendant Alexander P. Bebris with Distribution of Child Pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and Possession of Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The charges stem from Facebook's discovery that Bebris uploaded several child pornography images via Facebook Messenger in September 2018. Facebook relayed that information to the National Center for Missing and Exploited

Children (NCMEC), which then sent it to local law enforcement in Wisconsin. In December 2018, the Winnebago County Sheriff's Office (WCSO) obtained and executed a search warrant at Bebris' residence based on the information provided by NCMEC, where officers found additional child pornography files.

Currently before the court is Bebris' motion to suppress the evidence and statements obtained following the search of his residence. Bebris claims that his Fourth Amendment rights were violated when private entities and law enforcement reviewed the illegal images he allegedly uploaded to Facebook. More specifically, Bebris contends that Facebook and NCMEC were acting as agents of the Government when they identified and reviewed the child pornography files Bebris allegedly uploaded to Facebook and forwarded the information concerning the uploads to WCSO. An evidentiary hearing was

held on Bebris' motion on December 3, 2019, and the parties submitted both pre-hearing and post-hearing briefs. In addition, the court heard argument and reviewed briefing on Facebook's motion to quash the subpoena that Bebris' attorneys issued to it. For the reasons that follow, Bebris' motion to suppress will be denied and Facebook's motion to quash will be granted.

FINDINGS AND ANALYSIS

A. Expectation of Privacy

The evidentiary hearing and most of the argument and briefing centered on the issue of whether Facebook and NCMEC act as government agents in the investigation of child pornography. The more immediate question, however, is whether Bebris had a reasonable expectation of privacy in the Facebook messages he sent containing child pornography. I conclude he did not.

"[T]he application of the Fourth Amendment depends on whether the person invoking its protection can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotations omitted). "A defendant seeking to suppress the fruits of a search bears the burden of demonstrating both that he held an actual subjective expectation of privacy and that the expectation 'is one that society is prepared to recognize as reasonable.'" *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (quoting United *States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007)). While it appears clear, assuming the allegations in the Indictment are true, that Bebris had a subjective expectation of privacy in his Facebook email containing child pornography, i.e., he didn't think he'd be caught, his expectation was not objectively

reasonable in light of Facebook's published Community Standards and the terms of service he agreed to as a condition of opening a Facebook account.

Facebook is a well-known media company and electronic service provider ("ESP"). Facebook users create user names and can communicate with other Facebook users through, among other things, Facebook Messenger. Facebook has a corporate policy that prohibits content that sexually exploits or endangers children. Community Standards, Section 7: Child Nudity and Sexual Exploitation of Children, FACEBOOK, https://www.facebook.com/communitystandards/safety (last visited Mar. 5, 2020). The policy expressly warns users: "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." Id., Decl. of Michael Francis Xavier Gillin, II, ¶ 3, Dkt. No. 41 at 5. Facebook also discloses to its users that it collects data about "the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others." *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/update#legal-requests-prevent-harm (last visited Mar. 5, 2020). Users are told this information is used, inter alia, to "promote safety and security on and off of Facebook Products." Id. Among the third parties with whom users are told Facebook shares such information are law enforcement agencies. Facebook explains that "we access, preserve and share your information with regulators, law enforcement or others . . . [w]hen we

have a good-faith belief it is necessary to: detect, prevent or address . . . harmful or illegal activity." Id.

In the face of these disclosures, any expectation of privacy Bebris had with respect to child pornography uploaded via his Facebook Messenger account would be objectively unreasonable. See *United States v. Wilson*, No. 3:15-cr-02838-GPC, 2017 WL 2733879, at *7 (S.D. Cal. June 26, 2017) ("This express monitoring policy regarding illegal content, which Defendant agreed to, rendered Defendant's subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable."); *United States v. Ackerman*, 296 F. Supp. 3d 1267, 1273 (D. Kan. 2017) ("In this case, AOL's TOS [terms of service] similarly limits Defendant's objectively reasonable expectation of privacy. As noted above, the TOS informed Defendant that he must comply with applicable laws and that he

could not participate in illegal activities. AOL's TOS also informed Defendant that if he participated in illegal activities or did not comply with AOL's TOS, it could take technical, legal, or other actions without notice to him. Thus, the Court concludes that Defendant cannot establish a reasonably objective expectation of privacy in this particular email and its four attachments (containing child pornography) after AOL terminated his account for violating its TOS."); *United States v. Stratton*, 229 F. Supp. 3d 1230, 1242 (D. Kan. 2017) ("[B]ecause the Terms of Service Agreement reduced defendant's reasonable expectation of privacy in the information stored on his PS3 device, the court finds that the Fourth Amendment does not apply to Sony's search of defendant's images.").

This is not to say that, as a general matter, an individual's expectation of privacy in his or her own

email account is not reasonable. See *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("[W]e hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP.") (internal quotations omitted). In *Warshak*, the government used the Stored Communications Act (SCA), 18 U.S.C.§§ 2701 et seq., to compel an internet service provider (ISP) to disclose 27,000 of the defendant's private emails in the course of its investigation of a scheme to defraud predicated on the sale of an herbal supplement purported to enhance male sexual performance. Although some of the emails were incriminating, there was no allegation that they contained contraband. Moreover, the disclosure of the emails in *Warshak* was compelled by the government; it was not initiated by the ISP for its own purposes and in compliance with its terms of use.

Based on these facts, the court concluded that the government's conduct violated the defendant's Fourth Amendment rights. But neither *Warshak*, nor any of the other cases cited by Bebris, have held that one's expectation of privacy in child pornography sent via email is reasonable in light of the express disclosure by the ESP that such content is not allowed and will be reported to law enforcement. Such an expectation is not "one that society is prepared to recognize as reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967).

B. Facebook as Government Agent

Even if his expectation of privacy was reasonable, Bebris' motion would nevertheless fail because Facebook is not a government agent, and thus its actions in detecting the child pornography and sending the CyberTipline Reports to NCMEC were private actions not attributable to the government,

regardless of whether NCMEC is a government agent or not. The Fourth Amendment's purpose is to protect citizens against unreasonable searches and seizures by the government. It does not apply to searches or seizures performed by private individuals or entities unless they are acting as an instrument or agent of the government. In order to determine whether an individual was acting as a private party or as an "instrument or agent" of the government, courts look to "whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose in conducting the search was to assist law enforcement agents or to further its own ends." *United States v. Ginglen*, 467 F.3d 1071, 1074 (7th Cir. 2006) (internal quotations omitted). "Other useful criteria are whether the private actor acted at the request of the government and whether the government offered the private actor a reward." *Id.*

Here, the government neither knew of nor acquiesced in Facebook's monitoring of Bebris' emails. No law enforcement agency was investigating Bebris until NCMEC alerted WCSO that child pornography had been uploaded using his account. Of course, law enforcement is aware that Facebook and other ESPs monitor the content of messages sent using their products, just like it knows private mail carriers monitor packages for drugs, but this does not make ESPs or private carriers agents of the government. See *United States v. Koenig*, 856 F.2d 843, 850 (7th Cir. 1988) (holding that employee of Federal Express was not acting as a de facto government agent when he opened suspicious package and discovered cocaine, notwithstanding carrier's historical maintenance of good relations with law enforcement officials and employee's past cooperation with such officials, where employee was following carrier's own policy

authorizing search of suspicious packages for protection of itself and employees).

Facebook, like other ESPs have strong moral and business reasons of their own to prevent their products from being used to traffic in child pornography. No sane person, let alone a business that values its image and reputation, wants to be publicly associated with the sexual exploitation of children. As Facebook's Project Manager for Safety on its Community Operations team states in his declaration, "Facebook has an independent business purpose in keeping its platform safe and free from harmful content and conduct, including content and conduct that sexually exploits children." Gillin Decl. ¶ 3.

Other courts have recognized that other ESPs, like Facebook, have their own interest in preventing the use of their products to traffic in child

pornography and that laws mandating the reporting of child pornography to law enforcement do not transform them into government agents. See, e.g., *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010) ("We conclude that the statutory provision pursuant to which AOL reported Richardson's activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes."); *United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) ("[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."); *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) ("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."). As one

court recently noted, "district and circuit courts around the country . . . have universally rejected the arguments like Defendant's [that ESPs were acting as agents or instruments of the government in monitoring the email content of users and reporting suspected child pornography to NCMEC]." *United States v. Wolfenbarger*, Case No. 16-CR-00519-LHK-1, 2019 WL 6716357, at *12 (N.D. Cal. Dec. 10, 2019).

Bebris nevertheless argues that Facebook's cooperation with NCMEC, which is itself, in his view, an agent of the government, makes Facebook an agent of the government. He challenges the declarations filed by Facebook in support of its motion to quash the subpoena issued to compel its attendance at the evidentiary hearing held by the court and argues that he is entitled to live testimony, either in court or by video, to establish the close relationship between them.

To the extent Bebris' objection is to the admissibility of the declarations Facebook submitted, the objection is overruled. Bebris cites his Sixth Amendment right to compulsory process, but compulsory process is a trial right. It does not apply to pretrial proceedings. *Linder v. United States*, 937 F.3d 1087, 1090 (7th Cir. 2019) ("Compulsory process is a trial right; the Constitution does not entitle a criminal defendant to interview potential witnesses or take their depositions before trial."). Moreover, the Federal Rules of Evidence do not apply in full force to suppression hearings. Fed. R. Evid. 104(a), 1101(d)(1); see *United States v. Watson*, 87 F.3d 927, 30 (7th Cir. 1996) (holding that, "aside from privilege, exclusionary rules should not apply in a proceeding in which the court itself is considering the admissibility of evidence," including during suppression hearings) (citing *United States v. Matlock*, 415 U.S. 164, 173

(1974)); see also *United States v. Ozuna*, 561 F.3d 728, 736–37 (7th Cir. 2009) ("[T]he Rules of Evidence do not apply at pre-trial admissibility hearings. Rule 104(a) makes this explicit." (citations omitted)). As a result, Gillin's declarations are not excluded from consideration as inadmissible hearsay. The Court may receive the evidence and give it whatever weight it deserves. *Matlock*, 415 U.S. at 175.

To the extent Bebris' objection is that Facebook's declarations are not sufficient, the court concludes otherwise. Bebris' argument that NCMEC exceeded the scope of the private search conducted by Facebook is sufficiently addressed by Gillin's declaration describing the CyberTipline reports. Although the child pornography was originally identified by PhotoDNA, the computer program developed by Microsoft that allows ESPs, like Facebook, to more readily detect child pornography,

the images were viewed by a person before they were submitted to NCMEC, as reflected in the reports themselves. Supp. Decl. of Michael Francis Xavier Gillin, II, ¶ 7, Dkt. No. 53 at 5. This evidence refutes Bebris' argument that NCMEC expanded Facebook's search.

But even if no Facebook employee had viewed the files, the result would be the same. As the Fifth Circuit noted in *United States v. Reddick*, Microsoft's PhotoDNA relies on hash-values to identify child pornography, and "hash value comparison allows law enforcement to identify child pornography with almost absolute certainty, since hash values are specific to the makeup of a particular image's data." 900 F.3d 636, 639 (5th Cir. 2018) (internal quotations omitted). Thus, opening the files identified as child pornography by comparison of hash values would not be a significant expansion of a search previously

conducted by a private party such that it would constitute a separate search. Id.

Bebris' further argument that direct testimony by a Facebook executive is needed to determine the level of cooperation between Facebook and NCMEC is likewise unconvincing. Even if Facebook did receive training from NCMEC on the use of PhotoDNA and the process of filing CyberTipline reports so that it could more effectively monitor its products for child pornography and assist law enforcement, this would not transform Facebook into a government agent or instrumentality. See Koenig, 856 F.2d at 849 ("And the fact that the DEA may have aided Federal Express in the development of a drug shipper profile does not establish that Federal Express would use the profile at the government's behest, rather than for its own, private purposes. Presumably Federal Express would desire the best profile it could obtain, the better

to stem the tide of drugs shipped through its facilities. Use of an effective drug shipper profile, whatever its source, is consistent with a private business interest in protecting employees from contact with drug shipments.").

CONCLUSION

For these reasons, I conclude that Facebook's motion to quash Bebris' subpoena [Dkt. No. 40] should be granted. I further conclude from the evidence before me that Facebook was not acting as an agent or instrumentality of the government when it sent the CyberTipline reports to NCMEC identifying child pornography uploaded by Bebris' account via Facebook Messenger. And because Facebook acted independently, the court need not decide whether NCMEC is an agent of the government. Both because Bebris had no reasonable expectation of privacy in the child pornography depictions unloaded on his account

and because Facebook was not acting as an agent of the government, his motion to suppress [Dkt. No. 28] is denied. The Clerk is directed to place this matter on the court's calendar for a telephone conference with counsel to discuss further proceedings and, if necessary, schedule the matter for final pretrial and trial.

SO ORDERED at Green Bay, Wisconsin this 9th day of March, 2020.

s/ William C. Griesbach

William C. Griesbach, District Judge
United States District Court