UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA, v. MILTON WESTLEY, CLIFFORD BRODIE, SEDALE PERVIS, DEJUAN WARD, MICHAEL BELLE, MICHAEL VIA	No. 3:17-CR-171 (MPS)

RULING ON MOTIONS TO SUPPRESS EVIDENCE OBTAINED FROM FACEBOOK ACCOUNTS

I. Introduction

On August 3, 2017, following an investigation into several shootings in New Haven, a grand jury returned a multi-count indictment charging six individuals with various offenses, including RICO conspiracy, violent crimes in aid of racketeering ("VCAR"), offenses related to possession, transfer, and use of firearms, and possession with intent to distribute narcotics. (ECF No. 1 (charging violations of 18 U.S.C. 18 U.S.C. §§ 1962(d), 1959(a)(3) & (a)(5), 922 and 924, and 21 U.S.C. §§ 841(a)(1), 841(b)(1)(C), and 841(b)(1)(D)).)

Defendants Dejuan Ward, Clifford Brodie, and Michael Belle have filed motions to suppress evidence obtained from their respective Facebook accounts. (ECF Nos. 96, 104, and 121.) The Court held oral argument on these motions on April 10, 2018. For the reasons discussed below, the motions to suppress are DENIED.

II. Factual Background

A. The October 2016 Warrant

On October 11, 2016, Special Agent Brian Ross of the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") applied for and obtained from Magistrate Judge William I.

Garfinkel a warrant ("the October 2016 warrant") to search the contents of several Facebook accounts in connection with the investigation underlying the Indictment in this case.

The October 2016 warrant authorized a search of, among other accounts, "Account Four," bearing the Facebook User ID 100000756536727 and the user name "Go Brazy Doee (Top Opp Cliff)," allegedly used by Brodie; and "Account Seven," bearing the Facebook User ID 100002719106766 and user name "Don'Juan Hb Martinez," allegedly used by Ward. (An account allegedly used by Belle was the subject of a later warrant, as discussed below.) The warrant referred to an affidavit by Special Agent Ross, which was attached to the warrant application ("the October 2016 affidavit" or "Oct. 2016 Aff.").

Special Agent Ross's affidavit explained that ATF had been investigating what ultimately amounted to 40 shootings that occurred in New Haven throughout 2016. (Oct. 2016 Aff. ¶ 10.) Investigators believed that a number of those shootings were committed by members of a group known as the Goodrich Street Boys, or "GSB," and that individuals used Facebook to signify their membership in the group, including by referencing firearms, narcotics, and gang associations. (*Id*. ¶¶ 7-8, 10.) Special Agent Ross attested that probable cause existed to believe that the target accounts would contain direct evidence of drug trafficking, firearms offenses, and racketeering, and that those accounts would also yield evidence that GSB was an "enterprise" under the racketeering laws, as well as the identities of the members of the enterprise. (*Id*. ¶ 8.) *See* 18 U.S.C. § 1961(4) (defining "enterprise" to include any "group of individuals associated in fact although not a legal entity"). His affidavit indicates that some of the information it contains came from his review of publicly available portions of the target Facebook accounts. (*Id*. ¶ 9(a)-(g).)

Special Agent Ross described in the affidavit his experience as a law enforcement officer, including his specialized training in firearms identification and the investigation of firearms-

related offenses, his participation in investigations of firearms offenses, narcotics trafficking, and violent crimes, and his experience writing, obtaining, and coordinating the execution of search warrants. (*Id*. ¶ 1.) Special Agent Ross also described his experience investigating gangs and in executing search warrants involving electronic and social media, including Facebook accounts. (*Id*.) As a case agent investigating GSB, Special Agent Ross attested that he was personally familiar with the circumstances of the investigation underlying this case and the information contained in the affidavit. (*Id*. ¶ 3.)

1. Allegations With Respect to Brodie's Account

The October 2016 affidavit contained the following allegations directly related to Brodie and his Facebook account.

- Law enforcement believed Curtis Ratchford, a member of "Exit 8" and "an associate of FTP," or the "Fruit Town Piru street gang," a group associated with GSB, shot Damion Phillips, the leader of the rival "Slutwave" group on March 13, 2016, while attending the St. Patrick's Day parade in New Haven. Ratchford's Facebook records obtained earlier through a state search warrant revealed that he and others, including Brodie, using Account Four, had a group Facebook messenger conversation the next day in which they discussed the incident at the parade and a video that Michael Via, Brodie's co-defendant in this case, took during the incident. (*Id*. ¶ 13.) Brodie does not appear to have sent a message in the group conversation or to have been the subject of conversation, but others sent messages to him. (*See id.* ¶¶ 14-17.)
- On March 24, 2016, Ratchford posted a photograph on his Facebook page of him with Milton Westley, a defendant in this case, Brodie, and Robert Cook, another

individual whose Facebook account was a target of the October 2016 warrant. (*Id*. ¶ 21.)

- On July 14, 2016, after Via was arrested for a probation violation, he stated during an interview with law enforcement that he was "the leader of the G$B street gang," and "closely associated with Ratchford, Ward, Westley, and Brodie." (*Id*. ¶ 18.) Via admitted that there was an ongoing dispute between GSB and Slutwave. (*Id*. ¶ 18.) Via also admitted that he sells marijuana and that he uses his Facebook account and his cell phone to keep in contact with customers, which he had been doing for several years. (*Id*. ¶ 19.) Via said that he shared customers with other members of GSB. (*Id*. ¶ 19.)
- On July 27, 2016, Westley posted a photograph on his Facebook page of him with Cook, Ward, and Brodie. (*Id.* ¶ 22.)
- The same day, Ward posted a photograph on his Facebook page of him with Cook, Westley, and Brodie, with the caption, "HaPPy P day to my lil Pro," followed by "celebratory emojis." (*Id*. ¶ 25.) Based on his training and experience, Special Agent Ross alleged that the caption was meant to wish happy birthday to "one of his gang associates," but that by replacing the letter "b" with the letter "p," Ward was demonstrating his affiliation with the Piru street gang. (*Id*. ¶ 25.)
- On September 14, 2016, Brodie posted on his Facebook page, "Just got bro letter Curt Doee Free Burt." (*Id*. ¶ 24.) Based on his training and experience, Special Agent Ross believed this was a reference to Ratchford, who used the names "Curt Doee" and "Burt," and who was incarcerated at the time.

- Brodie posted a video on his Facebook page of him fighting with Dante Phillips, a member of Slutwave, on October 5, 2016. (*Id*. ¶ 24.)

2. Allegations with respect to Ward's Account

In addition to the above allegations involving Ward, Special Agent Ross alleged the following with respect to Ward and his Facebook account:

- On September 15, 2016, the day of a shooting involving alleged Slutwave members Jaison Flowers and Derrick Smith, the latter of whom suffered a gunshot wound, Ward posted messages on his Facebook page that Special Agent Ross interpreted to express that "rival Slutwave gang members were likely crying because Smith was shot," and that Slutwave "should go ahead and try to get even." (*Id*. ¶ 26.) Ward allegedly wrote, "Them nikkas prolyl over Thea crying n shit." Flowers allegedly responded to the post, "Never Crying Get Even," to which Ward replied, "Facts by all means handle/ Do ya thang baby do yo got dam thing." (ECF No. 96-1 ¶ 26.)
- On September 24, 2016, Ward posted a message that Special Agent Ross interpreted as "intended to mock the members of WR2/Slutwave by insinuating that they run from trouble rather than stand up and fight." (*Id*. ¶ 27.) Ward allegedly wrote, "Vill nikkas is the fastest nikkas in New Haven NBS Usain Bolt ain't got shit on em." (*Id*. ¶ 27.) Agent Ross interpreted "Vill nikkas" to be a reference to the rival "WR2/Slutwave" group, which allegedly congregates in the "Newhallville" section of New Haven, and includes the allegedly closely associated groups WR2 and Slutwave. (*Id*.)
- On October 3, 2016, Ward posted a photo on his Facebook page with a caption that Agent Ross interpreted as expressing Ward's belief that a fellow member of Fruit

Town Piru cooperated with law enforcement in order to get released from custody. (*Id*. ¶ 28.) The photo allegedly pictured an individual, with the face of fellow FTP member Otis Burton superimposed, walking into a police station. The caption read, "How snitches be looking when they have new info." Later the same day, Ward posted on his Facebook wall, "Kus up there in PC snitching and lying on mfs that was out here just boolin so he could kome home to bitch who doing dicks Otis one sick individual." (*Id*. ¶ 28.)

3. Additional Pertinent Allegations

The October 2016 Affidavit included other allegations regarding GSB members "closely associated" with Brodie and Ward (*Id*. ¶ 18) and the group's alleged drug activity:

- On March 28, 2016, Ratchford posted a photo on his Facebook page of bags containing what appeared to be marijuana. (*Id*. ¶ 21.)
- Via told law enforcement that he was at the St. Patrick's Day parade on the day of the shooting of Damion Phillips, and that Westley sent a group message to Via and others telling him he was in a fight with members with Slutwave. (*Id*. ¶ 18.) Via, Ratchford, and two other individuals went to meet Westley, where Via saw Westley punch a member of Slutwave and shortly after, heard gunshots. (*Id*.)
- On October 2, 2016, Westley posted on his Facebook page what Special Agent Ross believed were messages related to selling marijuana. (*Id*. ¶ 23.) Westley wrote, "Whose around late?" followed by a car emoji, cloud emojies, and the words "Hit me" with a phone emoji.

B. The August 2017 Warrant

On August 1, 2017, Special Agent Ross applied for and obtained from Magistrate Judge Holly B. Fitzsimmons a second warrant ("the August 2017 warrant") seeking updated account information for the accounts searched under the October 2016 warrant, including the accounts allegedly used by Brodie[1] and Ward, and seeking to search several additional Facebook accounts, including "Account Two," bearing the Facebook User ID 100000937575958 and user name "Chasingbenji MB," allegedly used by Defendant Michael Belle. This warrant referred to a second affidavit provided by Special Agent Ross ("the August 2017 affidavit" or "Aug. 2017 Aff.")

The August 2017 affidavit was substantially similar to the October 2016 affidavit but added certain allegations. The affidavit generally alleged that based on information gleaned from the search authorized by the October 2016 warrant, the ATF learned that "members and associates of GSB use Facebook to communicate with each other and with members of rival gangs," and that "GSB members and associates . . . use Facebook to threaten rival gang members." (Aug. 2017 Aff. ¶ 11.) With respect to Belle, the only one of the three moving defendants whose Facebook account was not also a target of the October 2016 warrant, the affidavit stated that Special Agent Ross had reviewed the "publicly available Facebook page" associated with Belle's account. (*Id.* ¶ 9(b).) Special Agent Ross further alleged that some of the communications between alleged GSB members and members of other groups occurred close in time to shootings law enforcement had linked to the groups using ballistics testing. (*Id.* ¶ 11.)

1. Allegations with respect to Ward's Account

Special Agent Ross alleged in the August 2017 affidavit that Ward's account was still active. (*Id.* ¶ 50.) Special Agent Ross provided the following additional allegations regarding Ward and his Facebook account:

[1] The user name associated with this account in August 2017 was "Chase a Check Cliff."

- Ward and Brandon Shealey, a member of Slutwave, had a conversation via Facebook Messenger that Ross interpreted to be about "an associate of Ward who had been disrespectful of Shealey." (*Id*. ¶ 18.) The conversation took place 19 days after a shooting in front of Shealey's house, which law enforcement believed GSB was involved in. (*Id*.)
- By reviewing Facebook records from an account belonging to Pharoh Jackson, another Slutwave member, law enforcement learned that on September 17, 2015, the day the government alleges in the Indictment that Ward shot Jackson in the leg, Jackson and Ward had a conversation via Facebook Messenger concerning the shooting earlier that day. (*Id*. ¶ 27.)

2. Allegations with respect to Brodie's and Belle's Accounts

Special Agent Ross alleged in the August 2017 affidavit that Brodie's account was still active. (*Id*. ¶ 9(l).) Special Agent Ross also alleged that Belle was a member of GSB and had a "close relationship" with Brodie and Westley, based on surveillance, interviews of witnesses, and previously obtained Facebook messages between Belle and other alleged GSB members. (*Id*. ¶ 15.) Special Agent Ross also provided the following allegations with respect to Brodie and Belle. Because the allegations involving either Brodie or Belle frequently involved both individuals, I discuss those allegations together.

- On January 1, 2016, Belle received messages in a Facebook group chat with Cook, Brodie, Via, and Westley, in which Cook sent a message that Special Agent Ross interpreted to mean that Cook was asking Westley if he should bring a gun somewhere. (*Id*.) Westley wrote, "Head come out in 5min," to which Cook replied, "Bring the pole or Na." (*Id*.)

- On January 13, 2016, Belle sent a message to Via that Special Agent Ross interpreted to mean that Belle wanted Via to tell Ward that Belle had a drug customer for Ward. (*Id*. ¶ 16.) Belle wrote to Via, "Yo I gotta trap fa hot Boi." (*Id*. ¶ 16.) Ward allegedly uses the name "Hot Boi."
- On January 22, 2016, two days after someone shot at Shealey's home, and one day before a second shooting at Shealey's home during which bullets traveled through a window and into Shealey's neighbor's bedroom, Shealey and Brodie had a Facebook conversation in which Brodie asked Shealey if he would Facetime with him. Brodie provided a Facetime account that, based on the email address associated with the account, appeared to be Belle's account, indicating that Brodie and Belle likely were together at the time. (*Id*. ¶ 20.) After the second shooting at Shealey's home, ATF agents learned that Belle sent a video of the shooting captured by Westley to Sedale Pervis, another alleged member of GSB and defendant in this case. (*Id*.)
- Brodie recorded on Facebook Live[2] a video depicting the February 6, 2016 shooting of Damien Smith on Munson Street. (*Id*. ¶ 33.)
- On March 5, 2016, Pervis, West, Brodie, Via, Cooke, and Ratchford participated in a group Facebook conversation that Special Agent Ross interpreted to discuss drug sales. (*Id*. ¶ 25.) Via wrote, "I'm Talking Bout Scope I Got A Trap For Him," to which Pervis replied, "I'm coming lil," with a "gas emoji" that Special Agent Ross

[2] Facebook Live is a feature provided by Facebook that allows users to share live video with their followers and friends on Facebook. After the live video ends, the video is published to the user's profile so that the user's Facebook friends can watch it at a later time. *See* https://live.fb.com/about/ (last accessed June 19, 2018).

believed is a symbol for "gang." Via then responded that he "got a jugg," which Special Agent Ross interpreted as a reference to a drug customer. (*Id*.)

- On April 27, 2017, Brodie recorded a Facebook Live video depicting him and Belle approaching an unmarked federal D.E.A. vehicle conducting surveillance in the area of 1070 Townsend Avenue, Brodie's and Westley's residence. The video showed Belle and Brodie yelling at the car and reading the license plate. (ECF No. 96-1 ¶ 48.)
- Brodie had a Facebook conversation with Pharoh Jackson after he attempted to call Jackson and Jackson did not answer. Brodie allegedly accused Jackson of being "police." (ECF No. 96-2 ¶ 29.)
- On June 27, 2017, Brodie posted to his Facebook page, "Keep your mouth shut during them investigations you'll be out the station n a dare or two." (*Id*. ¶ 48.) Brodie posted this one day after the NHPD and ATF engaged in a vehicle pursuit involving Brodie, Westley, and Belle. (*Id*.)

Special Agent Ross also alleged that he obtained on July 12, 2017 a warrant to search a cell phone seized from Brodie after police engaged him, Westley, and Belle in the vehicle pursuit. (*Id*. ¶ 17.) Upon reviewing the contents of Brodie's cell phone, Agent Ross learned that Brodie used Facebook Messenger to communicate with others using text messages and phone calls, and that Belle was one of Brodie's most recent and frequent contacts. (*Id*.)

3. Additional Pertinent Allegations

The August 2017 affidavit included additional allegations regarding the relationships between alleged GSB members, GSB's activities, and GSB's relationship with rival groups.

- On February 12, 2016, Via and alleged Slutwave member Dean Williams had a conversation that Special Agent Ross interpreted to be about a marijuana sale. (*Id*. ¶ 32.) Via wrote to Williams, "I'm Waiting For More Bud," which Special Agent Ross interpreted to mean that Via was waiting to be resupplied with marijuana. (*Id*.)
- On February 14, 2016, GSB members Pervis and Lamar Wooten had a Facebook conversation that Special Agent Ross also interpreted to be about a marijuana sale. (*Id*. ¶ 24.) Wooten wrote to Pervis, "y got bud," to which Pervis responded, "yeah call my phone." (*Id*.) Shortly after, Pervis told Wooten that he was "bout to be there" and to "come out". (*Id*.)
- On March 6, 2016, alleged Slutwave member Anthony Pritchett sent Via a private message referring to a song Pritchett wrote, in which he allegedly "named several GSB members and that he would shoot at them if given the opportunity." (*Id*. ¶ 16.) Pritchett's song referred to the February 6, 2016 shooting of Damien Smith on Munson Street and indicated that GSB was responsible for the shooting. (*Id*.)

III. Discussion

A. Reasonable Expectation of Privacy

A defendant seeking suppression "is obliged to show that he had a legitimate expectation of privacy . . . before he can invoke the protection of the Fourth Amendment." *United States v. Smith*, 621 F.2d 483, 486 (2d Cir. 1980). *See also Rakas v. Illinois*, 439 U.S. 128, 144 n.12 (1978) ("Legitimate expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."). Much of the information contained in Defendants' Facebook accounts was shared with third parties and, with respect to the publicly available portions

of the Facebook pages reviewed by Special Agent Ross in preparing the affidavits, with the public at large. I therefore begin by addressing whether Defendants had a reasonable expectation of privacy in the information authorized to be searched and seized by the warrants.

"Individuals generally possess a reasonable expectation of privacy in their home computers." *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004). "But this expectation is not absolute, and may be extinguished when a computer user transmits information over the Internet or by e-mail." *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (citing *Lifshitz*, 369 F.3d at 190). "A central element in determining whether an individual has a reasonable expectation of privacy is the effort made to keep the subject information private." *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 146 (E.D.N.Y. 2013).

Because of the nature of a Facebook account, which allows users to post information privately, share information with select groups of "friends," or post information publicly, courts have held that whether the Fourth Amendment applies to a user's Facebook content "depends, *inter alia*, on the user's privacy settings." *Meregildo*, 883 F. Supp. 2d at 525. *See also United States v. Khan*, No. 15-cr-00286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) (holding that defendant could not claim a Fourth Amendment violation where he "did not maintain any privacy restrictions on his Facebook account, and his Facebook profile was viewable by any Facebook user").

The defendants did not submit affidavits or other evidence showing that the Facebook accounts at issue even belong to them, and Brodie's motion pointedly refused to acknowledge that they did. (ECF No. 96 at 1-2 (referring to a Facebook account "allegedly utilized by Clifford Brodie" and stating that "the affidavit . . . does not disclose how this account is known to be used by Clifford Brodie, just that it is").) Nonetheless, defense counsel for Ward, Brodie, and Belle

acknowledged at oral argument that the relevant Facebook accounts belonged to them for the purposes of these motions, and I will thus assume that they did.

Defendants have not, however, provided affidavits or any other facts concerning the privacy settings on their Facebook accounts or any steps they took to keep their Facebook content private.[3] And it is not otherwise apparent from the record what, if any, privacy settings applied to those accounts. Indeed, at least some portions of the Facebook accounts were publicly available and were in fact reviewed by Special Agent Ross in preparing the affidavits. Further, much of the content of the accounts the affidavits refer to with respect to Ward, Brodie, and Belle was shared with third parties—including not only other defendants and alleged members of GSB but also alleged members of rival groups—through Facebook messages and posts.

To be sure, I can infer from the fact that the Government applied for the warrants in the first place and that the August 2017 affidavit contained additional information about Facebook content not present in the October 2016 warrant that not all of the Facebook content seized by the Government was publicly available. Nonetheless, an individual does not have to go so far as to broadcast information to the public at large to forfeit his claim to a reasonable expectation of privacy in that information. *See, e.g.*, *Chaney v. Fayette Cnty. Pub. Sch. Dist.*, 977 F. Supp. 2d 1308, 1316 (N.D. Ga. 2013) (holding that plaintiff "surrendered any reasonable expectation of privacy when she posted a picture to her Facebook profile, which she chose to share with the broadest audience available to her," i.e., when she chose the privacy setting of "friends and friends of friends"). There is a spectrum of privacy settings available on Facebook, and those settings can

[3] Brodie appears to concede that the Court would need more information regarding his privacy settings in order to conclude that he had a reasonable expectation of privacy over his Facebook account. (*See* ECF No. 96 at 10-11 (quoting *Meregildo*'s statement that "[w]hether the Fourth Amendment precludes the Government from viewing a Facebook user's profile absent a showing of probable cause depends, inter alia, on the user's privacy settings").)

be tailored to specific types of communications. Yet while the affidavit in this case describes a variety of such communications—video, wall postings, messages, etc.—the defendants have done nothing to show what, if any, privacy settings governed any of the types of communications found in their accounts. Defendants have therefore not established that they had a reasonable expectation of privacy in any of the communications described in the affidavits. *See Meregildo*, 883 F. Supp. 2d at 525 ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment."); *United States v. Adkinson*, No. 4:15-cr-00025-TWP-VTW, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017) (finding no reasonable expectation of privacy in messages defendant shared on others' Facebook pages); *United States v. Devers*, No. 12-CR-50-JHP, 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012) ("[U]nless the defendants can prove that their [F]acebook accounts contained security settings which prevented anyone from accessing their accounts, this court finds their legitimate expectation of privacy ended when they disseminated posts to their 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the government.").[4]

Because Defendants have not submitted any information regarding steps they took to keep their Facebook content private, they have not met their burden to demonstrate that they had a

[4] Some of the information authorized to be searched and seized was likely not shared with other Facebook users, such as Facebook security questions and answers, pending and rejected "Friend" requests, IP logs, records of Facebook searches performed, credit card or bank account numbers associated with the account, privacy settings, records showing which Facebook users had been blocked by the account, and records of communications with support services. Defendants have not pointed out, however, what, if any, such information was seized in this case. Nor have they provided the Court with any statements from which it could determine that they had a reasonable expectation of privacy in that information. And, as discussed below, courts have held that Internet users do not have a reasonable expectation of privacy in much of this information, such as logs of IP addresses.

reasonable expectation of privacy in any of the information searched.[5] Their motions fail on this ground alone. *See, e.g., United States v. Bedell*, 311 Fed. Appx. 461, 463, 465 (2d Cir. 2009) (noting that where the defendant "provided scant evidence to support the inference that he had a reasonable expectation of privacy in the common hallway," his "failure to demonstrate a reasonable expectation of privacy . . . sufficiently justifie[d] [the Second Circuit's] decision to affirm" the district court's denial of a motion to suppress).

Although Defendants' failure to demonstrate a reasonable expectation of privacy in their Facebook accounts is dispositive of their motions to suppress, I also address below whether the warrants were supported by probable cause, whether they were overbroad or lacked particularity, and whether the good-faith exception should apply.

B. Probable Cause

Defendants argue that the warrants were not supported by probable cause, and that the August 2017 warrant was tainted because it was procured with information obtained from the search authorized by the October 2016 warrant. I disagree.

Probable cause is a "flexible, common-sense standard." *Texas v. Brown*, 460 U.S. 730, 742 (1983). It merely requires the reasonable belief "that certain items may be contraband or stolen property or useful as evidence of a crime." *Id*. Courts "accord great deference to a judge's

[5] Neither Brodie nor Belle makes any arguments regarding his expectation of privacy in his Facebook account. Ward makes a passing reference to the Second Circuit's recognition that the Stored Communications Act embodies "an expectation of privacy in [personal electronic] communications, notwithstanding the role of service providers in their transmission and storage," *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 217 (2d Cir. 2016), *vacated and remanded by United States v. Microsoft*, 138 S.Ct. 1186 (2018), but also does not make any specific argument that he had a reasonable expectation of privacy in the particular information disclosed by Facebook or seized by the government.

determination that probable cause exists, and . . . resolve any doubt about the existence of probable cause in favor of upholding the warrant." *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998) (internal quotation marks omitted). The Court's "duty is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *Id.* (internal quotation marks and alterations omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983)). The "Fourth Amendment does not require probable cause to believe evidence will *conclusively* establish a fact, [but only that it] . . . *will aid* in a particular . . . conviction." *Messerschmidt v. Millender*, 565 U.S. 535, 552 n.7 (2012) (emphasis in original). Nonetheless, warrant applications may not rely merely on "conclusory statement[s]." *Illinois v. Gates*, 462 U.S. 213, 239 (1983).

1. October 2016 Warrant

Special Agent Ross's October 2016 affidavit established probable cause to believe that evidence of the crimes alleged in the Indictment would be found in Ward's and Brodie's accounts. The affidavit sets forth factual allegations that Ward, Brodie, and those with whom they communicated using Facebook were members of GSB and communicated about violent acts by members of GSB, establishing probable cause to believe that their Facebook accounts would contain evidence of a RICO conspiracy and VCAR offenses, among others.

First, the affidavit contains several allegations establishing probable cause to believe that Brodie and Ward were closely associated with other members of GSB. (*See, e.g.*, Oct. 2016 Aff. ¶ 18 (Via's statement to law enforcement that he was "the leader of the G$B street gang" and "closely associated with Ratchford, Ward, Westley, and Brodie"), ¶ 21 (discussing a photograph Ratchford posted on his Facebook page of him with Westley, Brodie, and Cook), ¶ 22 (discussing a photograph Westley posted on his Facebook page of him with Cook, Ward, and Brodie), ¶ 25 (discussing a photograph Ward posted on his Facebook page of him with Cook, Westley, and

Brodie with a caption referring to the "Piru" street gang).) *See United States v. Arnold*, No. 15-20652, 2017 WL 4036312, at *3 (E.D. Mich. Sept. 13, 2017) (denying a motion to suppress Facebook evidence of a RICO conspiracy and noting that "[t]he fact that the defendants posted photographs of themselves wearing gang clothing or posted statements that acknowledge the existence of, and their involvement with, the Seven Mile Bloods, their various monikers . . . , or statements referring to fellow co-conspirators by their gang names can be used by the government to demonstrate that this enterprise exists").

The October 2016 affidavit also established probable cause to believe that Brodie's and Ward's accounts would contain evidence of GSB's alleged violent acts, and that Brodie and Ward used their Facebook accounts to communicate with and about members of rival groups. For example, the October 2016 affidavit alleged that Brodie was one of a small group of individuals who received messages one day after the St. Patrick's Day parade shooting of Damion Phillips regarding the shooting, and that Ratchford, who was the alleged shooter, was part of the same group. (Oct. 2016 Aff. ¶¶ 13-17.) Special Agent Ross's allegations that Brodie participated with Ratchford in a Facebook discussion of Ratchford's alleged shooting of Damion Phillips and a video taken of the incident by Via, and that Brodie posted a video of himself fighting with Dante Phillips on October 5, 2016 (*Id.* ¶ 24), established probable cause to believe that Brodie's account would contain evidence of VCAR offenses. The allegations that on September 15, 2016, the day Derrick Smith, one of GSB's alleged rivals, was shot, Ward posted on his Facebook page that Slutwave members were crying because of the shooting and should try to get even, and later insinuated in a Facebook post that Slutwave members ran from trouble rather than fight (*Id.* ¶¶ 26-27) suggested, at least, that Ward had personal knowledge of the shooting and used Facebook to

taunt rival groups regarding specific instances of violence. That is enough to establish reason to believe that a search of Ward's account would yield further evidence of crimes of violence.

Further, although this is a closer call, the allegations that Via told law enforcement that he had been selling marijuana using his Facebook account for several years and shared customers with other members of GSB (*Id.* ¶ 19), combined with allegations of his association with Brodie and Ward and of Facebook posts and messages by other alleged GSB members referencing drugs and drug sales (*e.g.*, ¶ 21 (Ratchford posted a photo on his Facebook page of bags containing what appeared to be marijuana), ¶ 23 (Westley posted messages on his Facebook page that were believed to be related to selling marijuana)) also established probable cause that Brodie's and Ward's Facebook accounts would contain evidence of GSB's alleged drug activity.

Brodie argues that much of the Facebook information Special Agent Ross relied on to establish probable cause is "gibberish," and that Special Agent Ross did not sufficiently explain his interpretations of the information. But Special Agent Ross provides interpretations of each piece of information gathered from the Facebook accounts based on his training and experience. For example, Special Agent Ross attested that, based on his experience investigating street gangs, firearms offenses, and narcotics trafficking, he believed that "cloud" emojis referred to drugs (Oct. 2016 Aff. ¶ 23), and that "Vill nikkas" referred to Slutwave, because of its association with the Newhallville section of New Haven. (*Id.* ¶ 27.) It is well established that law enforcement agents may rely on their training in interpreting facts to establish probable cause. *See United States v. $557,933.89, More or Less, in U.S. Funds*, 287 F.3d 66, 85 (2d Cir. 2002) ("An officer's experience and training . . . are to be taken into account such that . . . a trained and experienced officer will have probable cause in circumstances when the layman would not.") (internal quotation marks omitted); *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985) ("[A]n agent's

expert opinion is an important factor to be considered by the judge reviewing a warrant application.").[6]

Brodie also asserts that the affidavits "establish nothing more than [he] is a member of GSB who happens to own a Facebook account." (ECF No. 96 at 13.) That assertion ignores the specific content regarding acts of violence—such as the St. Patrick's Day parade shooting—found in Brodie's account. Whether or not the affidavit establishes probable cause to believe that Brodie *committed* those acts of violence is beside the point, because the warrant authorized a search of Brodie's Facebook account, not his arrest. *See United States v. Rojas*, 671 F.2d 159, 165 (5th Cir. 1982) ("[T]he facts necessary to show probable cause to arrest are not necessarily the same as those required to show probable cause to search."). An affidavit need not allege that a defendant committed an illegal act to establish probable cause. *United States v. Martin*, 426 F.3d 68, 76 (2d Cir. 2005) ("probable cause does not require a prima facie showing" of criminality). Rather, it must, when "viewed through the lens of common sense," demonstrate that a "reasonably prudent person [would] think that a search [of Brodie's and Ward's Facebook accounts] would reveal . . . evidence of a crime." *Florida v. Harris*, 568 U.S. 237, 248 (2013). The October 2016 affidavit meets that standard.

2. August 2017 Warrant

Because probable cause supported the October 2016 warrant with respect to the Facebook accounts of Brodie and Ward, the August 2017 warrant was not tainted due to its use of information

[6] Brodie relies on *United States v. Bethal*, 245 Fed. Appx. 460 (6th Cir. 2007), a summary order in which the Sixth Circuit held that a warrant lacked probable cause because there was an insufficient nexus between the place to be searched—in that case, the suspect's residence—and the two shootings law enforcement suspected the defendant was connected to. *Id*. at 468-69. *Bethal*'s reasoning does not apply here, as there is ample evidence, as discussed above, connecting offenses involving violence and drugs to the place to be searched, Ward's and Brodie's Facebook accounts.

procured by the earlier warrant. *See, e.g.*, *United States v. Cyr*, No. 2:14-cr-19, 2014 WL 6386805, at *4 (D. Vt. Nov. 14, 2014) (holding that one Facebook warrant was an "independent source of probable cause" for a broader, second Facebook warrant).

The August 2017 warrant independently established probable cause with respect to Belle's Facebook account, which was not a target of the October 2016 warrant. The affidavit alleged that Belle received messages in a group conversation with GSB members Cook, Brodie, Via, and Westley, which Special Agent Ross interpreted to be about carrying a gun. (Aug. 2017 Aff. ¶ 15 (alleging that Westley told Cook in the group conversation, "Head come out in 5min," to which Cook replied, "Bring the pole or Na").) The affidavit also alleged that Belle wrote to Via, "Yo I gotta trap fa hot Boi," which Special Agent Ross interpreted to mean that Belle had a drug customer for Ward. (*Id*. ¶ 16.) The affidavit also alleged that Brodie, Westley, and Belle engaged the police in a vehicle pursuit, after which law enforcement had obtained a search warrant for Brodie's phone, and that, based on the material recovered from the phone, Special Agent Ross learned that Brodie used Facebook to communicate through texts and phone calls, and did so particularly frequently and recently with Belle. (*Id*. ¶ 17.) All of these allegations demonstrated probable cause that Belle's Facebook account would contain evidence of firearms and drug trafficking offenses, and that Belle used his Facebook account to communicate with other members of GSB, with whom he was closely associated.

The August 2017 warrant also independently established probable cause with respect to Brodie's and Ward's accounts. The allegation that Brodie posted a Facebook Live video depicting the February 6, 2016 shooting of Damien Smith supplied probable cause to believe that his account would contain evidence related to the shooting. (*Id*. ¶ 33) The allegation that on September 17, 2015, the day the government alleges Ward shot Pharoh Jackson in the leg, Ward and Jackson

discussed the shooting via Facebook Messenger—which law enforcement learned from a review of Jackson's Facebook account—established probable cause to believe that Ward's account contained evidence linked to the shooting. (*Id.* ¶¶ 26-27.) Thus, I find that both the October 2016 and August 2017 warrants were supported by probable cause as to the accounts of Brodie, Ward, and Belle.

C. Particularity and Overbreadth

Ward and Belle further argue that the warrants were overbroad and lacked particularity.[7] Specifically, they argue that the warrants violated the Fourth Amendment because they required Facebook to turn over the entirety of Defendants' accounts to the government without providing adequate guidance about what to search for, authorized the government to seize broad categories of information, and failed to provide a temporal limitation for the information to be searched or seized. I discuss below additional facts concerning the October 2016 and August 2017 warrants to provide necessary context for this argument.

The October 2016 warrant application sought to search seven Facebook accounts identified by their Facebook user ID numbers, listed in Attachment A. It also sought disclosure of the following information associated with each account, listed in Section I of Attachment B:[8]

[7] Brodie challenges the warrants on the sole ground that they failed to establish probable cause to search his Facebook account and makes no arguments regarding overbreadth or particularity. (ECF No. 96.) Belle adopts the arguments made in Ward's and Brodie's motions with respect to the August 2017 warrant, and adds an overbreadth argument similar to one of Ward's, i.e., that "the warrant sought content from his Facebook account going back to at least September 2010, when [he] was 12 years old." (ECF No. 121-1 at 2.) I address this argument below.

[8] The Government described at oral argument the process it used to execute these search warrants. According to the Government, after it served Facebook with the warrants, Facebook granted the Government online access to a secure server, after which the Government downloaded each category of information for which the warrant authorized disclosure. Because of the vast amount of data involved, the download process took days.

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(1) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account; and

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The October 2016 warrant application further sought authorization to seize the following information for each account, listed in Section II of Attachment B:

(a) All information that constitutes fruits, evidence and instrumentalities of conduct that would give rise to violations of 18 U.S.C. §§ 924, 1959, and 1962, and/or 21 U.S.C. § 841(a)(1), including, but not limited to, photographs and videos; the content of messages, chats, comments, and other communications; friend lists; "likes"; and location information, e.g., IP logs and "check ins";

(b) Transactional information of all activity of the accounts, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

(c) Business records and subscriber information, in any form kept, pertaining to the account, including applications, subscriber's full name, all screen names associated with the subscriber and/or account, all account names associated with the subscriber, telephone numbers, and addresses;

(d) Records indicating the services available to the subscriber of the accounts;

(e) Records relating to who created or used the Account, including records that help reveal the whereabouts of such person(s); and

(f) Records relating to the identity of the person(s) who communicated with the user of the account about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

The August 2017 warrant authorized the disclosure, search, and seizure of substantially similar information, also listed in Attachment A and Sections I and II of Attachment B.

* * *

The particularity requirement and prohibition against overbreadth stem from the language of the Fourth Amendment, which provides that "no Warrants shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., amend. IV. "Although somewhat similar in focus, [overbreadth and particularity] are two distinct legal issues: (1) whether the items listed as 'to be seized' in the warrant were overbroad because they lacked probable cause and (2) whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers." *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013) (internal quotations omitted). I address below the related but distinct issues of particularity and overbreadth.

1. Particularity

The particularity requirement has three components. First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes. *United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013). The requirement ensures "the rational exercise of judgment in selecting what items to seize." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000). Particularity concerns arise "when a warrant's description of the place to be searched or the items to be seized is so vague that it fails reasonably to alert executing officers to the limits of their search and seizure authority." *United States v. Scully*, 108 F. Supp. 3d 59, 90 (E.D.N.Y. 2015).

"In the Second Circuit, there is no settled formula for determining whether a warrant lacks particularity." *Zemlyansky*, 945 F. Supp. 2d at 453. "[W]arrants will frequently lack particularity where they include a general, catch-all paragraph or provision, often one authorizing the seizure of any or all records of a particular type," such as "any papers, things or property of any kind" or "all business records." *United States v. Vilar*, No. 05 Cr. 621, 2007 WL 1075041, at *22 (S.D.N.Y. Apr. 4, 2007) (quoting *United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987); *United States v. Hickey*, 16 F. Supp. 2d 223, 240 (E.D.N.Y. 1998)). "[C]ourts have [also] found warrants for the seizure of records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether." *United States v. Cohan*, 628 F. Supp. 2d 355, 365-66 (E.D.N.Y. 2009). The Second Circuit, however, has "not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants." *Galpin*, 720 F.3d at 451.

The October 2016 and August 2017 warrants identified the specific offenses for which the affidavits established probable cause. (*See, e.g.*, October 2016 Warrant, Attachment B, Section

II(a) (authorizing seizure of "[a]ll information that constitutes fruits, evidence and instrumentalities of conduct that would give rise to violations of 18 U.S.C. §§ 924, 1959, and[]1962, and/or 21 U.S.C. § 841(a)(1)"); October 2016 Warrant Application (specifying that the search was related to a violation of 18 U.S.C. §§ 924 and 1959); Oct. 2016 Aff. ¶ 2 (defining racketeering conspiracy, violent crimes in aid of racketeering, use of firearms in furtherance of violent crimes, and distribution and possession with intent to distribute narcotics as the "Subject Offenses"), ¶ 8 (Special Agent Ross's belief "that certain of the Target Facebook Accounts will contain direct evidence of drug trafficking, firearms offenses, and racketeering"); August 2017 Warrant, Attachment B, Section II(a) (authorizing seizure of the same categories of information as authorized by the October 2016 Warrant); Aug. 2017 Aff. ¶¶ 2, 8 (providing the same allegations as those provided in the October 2016 Affidavit regarding the Subject Offenses).) *See also United States v. Hernandez*, No. 09 Cr. 625, 2010 WL 26544, at *10 (S.D.N.Y. Jan. 6, 2010) (finding that a warrant was sufficiently particularized as to the underlying offenses where it referred to categories of documents related to particular statutes in Attachment B).

They also described the place to be searched—the particular Facebook accounts, identified by user ID number and user name in Attachment A. The fact that the accounts themselves contained a wide range of potentially relevant information does not mean that the warrants violated the particularity requirement. "A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement." *United States v. Ulbricht*, 858 F.3d 71, 102 (2d Cir. 2017) (holding that, where the defendant used his laptop to run a criminal enterprise, a broad warrant allowing the government to search defendant's laptop, Google account, and Facebook account was constitutional because the warrants were supported by probable cause and met all three

particularity requirements). Further, the warrants in this case went beyond identifying specific accounts to be searched by describing specific categories of information to be disclosed by Facebook to the government. (*E.g.*, "[a]ll contact and personal identifying information," "[a]ll activity logs," "[a]ll photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them," "[a]ll profile information," etc. *See* Attachment B, Section I.) The warrants thus easily satisfy the second element of the particularity requirement.

Ward argues that the warrants failed the third element—that they specify the items to be seized by their relation to designated crimes. Ward, and to some extent Belle, raise two concerns: the lack of any limitation on the types of information to be disclosed by Facebook, and the lack of any temporal limitation, each of which I address below.

Ward argues that "the warrant fails to place limitations on the type of private material to be reviewed, allowing a wholesale review of everything and anything." (ECF No. 104-1 at 8.) Ward is correct that the information to be disclosed by Facebook and reviewed by the government is extremely broad, and it is difficult to imagine a category of information associated with Defendants' Facebook accounts that the list of items to be disclosed does not capture. But the comprehensive list of items to be *disclosed* by Facebook did not authorize the *seizure* of those broad categories of information. The list of items to be seized by the government provided in Section II is much narrower and must be analyzed separately. And the disclosure of broad categories of information, to be searched later with specific queries yielding information to be seized, is a practical necessity when dealing with electronic evidence. "[A] search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search." *In the Matter of a Warrant for all Content and Other Information Associated with the Email Account xxxxxx@gmail.com*, 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) (holding that a search warrant

directing Google to provide the full content of a specified email account to the government was reasonable). "It has long been perfectly appropriate to search the entirety of a premises or object as to which a warrant has issued based on probable cause, for specific evidence as enumerated in the warrant, which is then to be seized." *United States v. Ulbricht*, No. 14-cr-68 (KBF), 2014 WL 5090039, at *14 (S.D.N.Y. Oct. 10, 2014), *aff'd*, 858 F.3d 71 (2d Cir. 2017). Thus, courts use "a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness." *Id*. *See also United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack.").

The Advisory Committee Notes to Rule 41 of the Federal Rules of Criminal Procedure, which refers to "later off-site copying or review," recognize the need for initially obtaining broad categories of electronic information that can later be queried for evidence of crimes falling within the warrant's scope:

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Fed. R. Crim. P. 41(e)(2) advisory committee's note to 2009 amendment. *See also United States v. Pugh*, No. 15-CR-116 (NGG), 2015 WL 9450598, at *27 (E.D.N.Y. Dec. 21, 2015) (holding that "the fact that the search allowed for the temporary seizure of the entire Facebook account [did] not render the search invalid"); *Meregildo*, 883 F. Supp. 2d at 526 (rejecting defendant's argument

that a Facebook warrant was invalid because "the Government did not employ any minimization procedure," noting that an attachment to the affidavit described that "the Government sought to seize information related to the scheduling of meetings among members of the racketeering enterprise, drug trafficking activity, and weapons," and that "[t]his description was sufficiently particular to allow the Government to examine the files it received from Facebook without violating the Fourth Amendment."). Therefore, the warrants' provisions requiring Facebook to turn over most or all of the information associated with the Defendants' accounts to the government, to be searched for specific categories of evidence to be seized, were reasonable and did not render the warrants insufficiently particular.

The warrants also sufficiently identified the items to be seized by relation to designated crimes in Attachment B, Section II. Section II(a) of both warrants authorized law enforcement to review the records produced by Facebook in order to locate "[a]ll information that constitutes fruits, evidence and instrumentalities of conduct that would give rise to violations of 18 U.S.C. §§ 924, 1959, and[]1962, and/or 21 U.S.C. § 841(a)(1), including, but not limited to, photographs and videos; the content of messages, chats, comments, and other communications; friend lists; 'likes'; and location information, e.g., IP logs and 'check-ins'." The warrants thus limited the seizures to evidence of violations of the criminal statutes at issue and provided an illustrative list of the items to be seized, a framework courts have held meets the third particularity requirement. *See United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990) (upholding a warrant containing "broadly worded categories of items available for seizure"); *United States v. Jacobson*, 4 F. Supp. 3d 515, 524 (E.D.N.Y. 2014) (holding that a "reference to particular offenses and the use of an illustrative list of items to seize sufficiently particularized the warrants"); *United States v. Bonczek*, No. 08-CR-361 (PAC), 2008 WL 4615853, at *12 (S.D.N.Y. Oct. 16, 2008), *aff'd*, 391 Fed. Appx. 21 (2d Cir.

2010) (upholding a warrant as sufficiently particular where "the warrant[s] listed various examples of the items to be seized," and "identified a specific illegal activity tied to the items that the Court authorized for seizure").

More specifically, courts in the Second Circuit have recently found warrants authorizing the seizure of broad categories of information from Facebook accounts to be sufficiently particular when the government sought to seize information related to particular offenses. *See, e.g.*, *United States v. Liburd*, No. 17-CR-296 (PKC), 2018 WL 2709199, at *2 (E.D.N.Y. June 5, 2018) ("Courts in this Circuit have found warrants that allow a Facebook search limited by reference to an exemplary list of items to be seized and the crime being investigated to be sufficiently particularized.") (internal quotation marks omitted); *Pugh*, 2015 WL 9450598, at *26 (finding that a search warrant for defendant's Facebook account was sufficiently particular where it limited the search by reference to an illustrative list of items to be seized and the crimes being investigated); *Meregildo*, 883 F. Supp. 2d at 526 (S.D.N.Y. 2012) (same). I find no meaningful differences between the limitations used in those cases and those here.

I note that the warrants also authorized the seizure of five additional categories of information listed Attachment B, Section II(b)-(f). Those categories of information concern identifying information and other "meta-data" related to the target accounts (such as the date an item was posted), however, rather than the content of the account. (*See e.g.*, "[t]ransactional information . . . including log files, dates, times, methods of connecting," "[b]usiness records and subscriber information," including "subscriber's full name, all screen names associated with the subscriber and/or account," "[r]ecords indicating the services available to the subscriber," "[r]ecords relating to who created or used the Account," and "[r]ecords relating to the identity of the person(s) who communicated with the user of the account about matters relating to the Subject

Offenses.") Because these categories do not concern the content of the accounts, it is not clear that law enforcement could have more particularly identified them in relation to the designated crimes. Nonetheless, as discussed above, paragraph (a) immediately preceding these categories identifies the relevant crimes, and paragraph (f) refers to the "Subject Offenses." I therefore find that the October 2016 and August 2017 warrants were sufficiently particularized with regard to the items to be seized in relation to designated crimes.

In any event, it is not clear that the defendants would have a reasonable expectation of privacy in the non-content items in the seizure list, assuming they had such an expectation in their Facebook accounts at all. *See supra*. Courts of Appeals have drawn a distinction between the content of Internet communications and subscriber information, holding that a defendant does not have a legitimate expectation of privacy in subscriber information disclosed to an Internet provider, such as IP address information. *See Ulbricht*, 858 F.3d at 97 (joining other circuits and holding that "collecting IP address information devoid of content is constitutionally indistinguishable from the use of a pen register," and therefore did not implicate the Fourth Amendment) (internal quotation marks omitted); *United States v. Graham*, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that "third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection"); *United States v. Wheelock*, 772 F.3d 825, 828 (8th Cir. 2014) (holding that the defendant could not claim an expectation of privacy in his subscriber information, including identifying information such as his IP address and name). Other courts have similarly held that defendants lack a reasonable expectation of privacy in subscriber information analogous to the information listed in Section II, paragraphs (b) through (f). *See, e.g.*, *United States v. Hammalian*, No. 2:17-CR-00070, 2018 WL 1951201, at *3 (D. Vt. Apr. 24, 2018) (denying a motion to suppress "subscriber information from

internet providers Google and Comcast, including the account holder's name, billing and email addresses, telephone number, services used, account creation date and status, login information, account identification number, IP addresses and history, and MAC addresses").[9]

Missing from both warrants, however, is a temporal limit on the information to be seized. Belle and Ward argue that without such a limit, the warrants authorized a search of content from their Facebook accounts going back to at least September 2010, when Belle was twelve years old, and, in Ward's case, to at least 2011, when he was fourteen years old. (ECF Nos. 104-1 at 8 and 121-1 at 2.). Although the lack of a temporal limit in a warrant may implicate both particularity and overbreadth, I analyze the issue under the rubric of overbreadth, as the principal thrust of Defendants' argument is that the warrants authorized a search of some material for which probable cause did not exist. (ECF No. 104-1 at 9 ("The warrants fail to limit the items subject to seizure by reference to any relevant timeframe or dates of interest, despite the affidavit categorically stating that the investigation involved certain shootings and assaults beginning in 2016.").[10]

---

[9] The Supreme Court recently held in *Carpenter v. United States* that an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements captured through cell-site location information, despite the individual's disclosure of that information to his wireless carrier. 138 S.Ct. 2206, 2217 (2018). Though defendants might argue that *Carpenter* casts doubt on whether the third-party doctrine negates an individual's expectation of privacy in Facebook account subscriber information, the Supreme Court was explicit that its holding was a "narrow one" and was not intended to disturb the third-party doctrine as applied to other technologies or "other business records that might incidentally reveal location information." *Id*. at 2220. The Supreme Court explained that its reasoning was based, in part, on the "unique nature of cell phone location information," *id*., in that it provided "encyclopedic" information about a person's past movements. *Id*. at 2216. No court appears to have held, and I do not find here, that Facebook account subscriber information implicates the concerns raised in *Carpenter*.

[10] Though I find that in this case, the lack of a temporal limit implicates the breadth of the warrant, some courts have discussed the issue under the rubric of particularity. *See, e.g., Jacobson*, 4 F. Supp. 3d at 526 (finding that "the absence of a time frame did not render the otherwise particularized warrants unconstitutionally general"); *United States v. Costin*, No. 5 Cr. 38, 2006 WL 2522377, at *12 (D. Conn. July 31, 2006) ("[a] warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may

2. Overbreadth

That the warrants ultimately authorized the government to seize information dating back years—back to when some of the Defendants were adolescents and before any of the criminal activity alleged in the affidavits began—concerns primarily the breadth of the warrants. *See United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009) ("Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based."); *United States v. Dinero Express, Inc.*, No. 99 CR 975 SWK, 2000 WL 254012, at *9 (S.D.N.Y. Mar. 6, 2000) ("When a warrant is challenged as overbroad, the issue is whether there exists probable cause to support the breadth of the search that was authorized."). "In other words, a warrant is overbroad if its 'description of the objects to be seized . . . is broader than can be justified by the probable cause upon which the warrant is based.'" *United States v. Romain*, No. 13-CR-724 (RWS), 2014 WL 6765831, at *7 (S.D.N.Y. Dec. 1, 2014) (quoting *United States v. Gamin*, 720 F.3d 436, 446 (2d Cir. 2013)); *Hernandez*, 2010 WL 26544, at *9 ("A failure to indicate a time frame could render a warrant constitutionally overbroad because it could allow the seizure of records dating back arbitrarily far and untethered to the scope of the affidavit which ostensibly provided probable cause.").

The focus of the affidavits is a series of shootings occurring in 2016, and the affidavits include only a few specific allegations dating back earlier. The October 2016 affidavit sets forth Special Agent Ross's description of a custodial interview with Michael Via, a co-defendant in this case, in which Via admitted that he sells marijuana, that he does so using Facebook and his cell

render it insufficiently particular."); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 58 (D. Conn. 2002) (finding a warrant sufficiently particular where it contained a "reasonably particular description of the items to be seized in the context of" a public corruption case, despite the lack of a temporal limitation).

phone, that he and other GSB members share customers, and that "he had been selling marijuana in this manner for several years." (*Id*. ¶19.) The August 2017 affidavit provided specific allegations regarding events dating back to September 17, 2015, the day the government alleges Ward shot Pharoh Jackson in the leg. (*See* Aug. 2017 Aff. ¶¶ 10-51.)[11]

Nonetheless, the information set forth in the affidavits does not establish a clear temporal cut-off, and it is not apparent how such a limitation would be drawn in this case. For example, as noted above, the affidavits establish probable cause to search for subscriber information, information about the creation of the target accounts, and information about the length of time the defendants and other GSB members have associated with one another. *See Boyle v. United States*, 556 U.S. 938, 946 (2009) (holding that a RICO "'enterprise' must have some longevity, since the offense . . . demands proof that the enterprise had 'affairs' of sufficient duration to permit an associate to 'participate' in those affairs through 'a pattern of racketeering activity'"). Much of that information likely dates back well before 2016, and it is not clear what date restrictions, if any, should have applied to such information. It would also be difficult to craft date restrictions for certain other content for which the affidavits plainly establish probable cause, e.g., items originally created or posted years ago but re-posted or sent immediately after a shooting in 2016, or references to drug dealing by Via and his sharing of drug customers with other GSB members. Further, the offenses that were the subject of the affidavit were not "single-act" crimes but instead consisted at least in part of complex offenses of broad scope, such as RICO conspiracy, which is an ongoing offense requiring proof of a "continuing" enterprise. *See Boyle*, 556 U.S. at 948 ("an

[11] The government represented at oral argument that it plans to introduce Facebook evidence from before 2016 at trial because the indictment alleges that Defendants' conspiracy began in approximately 2013 (ECF No. 1 ¶ 9), and in particular that Defendants' drug trafficking dated back several years, while the violent acts, with the exception of the alleged shooting of Pharoh Jackson, occurred in 2016.

association-in-fact enterprise is simply a continuing unit that functions with a common purpose"); *see also Hernandez*, 2010 WL 26544, at *9 ("Unlike in more straightforward 'single-act' criminal cases, a time-frame is less relevant to a warrant's breadth where the criminal acts are complex and necessarily extend over a significant period of time.").[12]

I conclude, however, that I need not resolve the issue of whether some date restriction was required and, if so, how it should have been framed, because I find below that the good-faith exception applies and thus that suppression is not warranted in this case.

D. Good-Faith Exception

Even if the absence of a date restriction made the warrants overbroad, I would still have to determine whether suppression is required. "The fact that a Fourth Amendment violation occurred—i.e., that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). Under the Supreme Court's holding in *United States v. Leon* recognizing a "good-faith" exception to the exclusionary rule, "[w]hen police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." *Herring*, 555 U.S. at 142 (quoting *Leon*, 468 U.S. 897, 922 (1984)).

[12] The Eleventh Circuit recently found that Facebook warrants were unnecessarily broad because they "required disclosure to the government of virtually every kind of data that could be found in a social media account," and were not limited to any time period. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017). The concerns expressed in *Blake* do not necessarily apply here, however, as the crimes in that case, child sex trafficking and conspiracy to sex traffic children, were more temporally circumscribed than the broad conspiracy alleged here. *See id*. at 974 (noting that the Facebook warrants "could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers" and "should have requested data only from the period of time during which [the defendant] was suspected of taking part in the prostitution conspiracy"). In any event, *Blake* ultimately held that the good-faith exception applied and refused to suppress the evidence obtained through the Facebook warrants. I reach the same conclusion as to the good-faith exception below.

"The good faith exception's requirement that an officer act with 'objective reliance' on a magistrate's warrant demands only that the officer exhibit reasonable knowledge of what the law prohibits." *United States v. Raymonda*, 780 F.3d 105, 119 (2d Cir. 2015). "Thus, to assert good faith reliance successfully, officers must, *inter alia*, disclose all potentially adverse information to the issuing judge." *United States v. Ganias*, 824 F.3d 199, 221 (2d Cir. 2016) (en banc).

Unlike in cases in which district courts have found that the good faith exception could not save unconstitutionally broad warrants, any deficiency here does not implicate "the fundamental and venerable prohibition on general warrants," of which all reasonable officers should be aware, as the warrants here did not include prohibited "catch-all language." *Cioffi*, 668 F. Supp. 2d at 397; *United States v. Vilar*, 2007 WL 1075041, at *23-24 (holding that a warrant that included "catch-all language"—i.e., language authorizing the seizure of all "corporate records" "includ[ing]" but "not limited to" particular categories of items—in the wake of clear Second Circuit precedent prohibiting such language was not objectively reasonable). Rather, any deficiency in the warrants in this case concerns nuances about searching social media accounts that a reasonable officer may not have yet confronted. *See, e.g.*, *Blake*, 868 F.3d at 974-75 (applying the good faith exception where the Facebook warrants were supported by probable cause, and whether they violated the particularity requirement was "not an open and shut matter" in light of the differences between searching social media information and searching a hard drive).

Indeed, the application of search warrants to Facebook accounts is a relatively new area of the law. In 2016, the Second Circuit discussed in *United States v. Ganias* differences between computer hard drives and physical files to provide guidance to courts on the constitutional parameters of digital searches. 824 F.3d 199, 211-14 (2d Cir. 2016) (en banc). By contrast, courts have yet to delve fully into the complexities of the application of the Fourth Amendment to social

media. *See e.g.*, *Ulbricht*, 858 F.3d at 104 (upholding search warrants for defendant's Google and Facebook accounts for substantially the same reasons as the Court upheld a search warrant for defendant's laptop, but without separate examination of the unique features of social media); *Blake*, 868 F.3d at 974 (querying, but not deciding, whether case law involving seizures of entire hard drives apply to the social media context). In particular, courts have yet to fully consider whether analogies to paper files and hard drives necessarily extend to social media, which is less private and more dynamic but also creates less of a concern for hiding evidence that has animated decisions about paper files and other digital media. *See Blake*, 868 F.3d at 974. They have also yet to explore whether and how to require date restrictions on dynamic content of the type found in social media accounts—especially in cases involving complex, ongoing crimes.

Because of these largely unexplored nuances in the application of the Fourth Amendment to Facebook accounts, and because the information in the affidavits that establishes probable cause is not demarcated by a clear date cut-off, I find that the good faith exception applies to the warrants at issue to the extent they are overbroad, and that suppression is unwarranted as a result. *See, e.g.*, *United States v. Levin*, 874 F.3d 316, 323 (1st Cir. 2017) (applying the good-faith exception to a warrant authorizing the government's use of "Network Investigative Technique" software, as the government, "[f]aced with the novel question of whether an NIT warrant can issue—for which there was no precedent on point—. . . turned to the courts for guidance," and reasoning that "such conduct should be encouraged, because it leaves it to the courts to resolve novel legal issues"); *United States v. Whitt*, No. 1:17CR060, 2018 WL 447586, at *4 (S.D. Ohio Jan. 17, 2018) (applying the good-faith exception to a Facebook warrant that failed to establish a nexus between the suspect's Facebook account and the items to be seized, noting that, [w]hile Sixth Circuit

jurisprudence on residential and other searches of a suspect is well-developed, Sixth Circuit jurisprudence on searching the Facebook account of a suspect is less so").

IV. Conclusion

For the reasons discussed above, Brodie's motion to suppress (ECF No. 96), Ward's motion to suppress (ECF No. 104), and Belle's motion to suppress (ECF No. 121) are DENIED.

IT IS SO ORDERED.

/s/
Michael P. Shea, U.S.D.J.

Dated: Hartford, Connecticut
July 17, 2018