



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF GEORGIA

AUGUSTA DIVISION UNITED STATES OF AMERICA UNITED STATES OF AMERICA)

v.) CR 117-035

ANTHONY TYRONE ROPER) GEORGE MACK BIRD, III AUDRA ROPER) AU

_____ The superseding indictment charges Defendant Anthony Tyrone Roper with procurement integrity fraud and bribery, Defendant Audra Roper with accessory after the fact, and both Defendants with making a false statement and obstructing justice. (Doc. no. 83.) Defendants move to suppress evidence seized pursuant to a search warrant for the Comcast email account quadar@comcast.net. (Doc. no. 50.) Upon consideration of the briefs and hearing testimony on January 24, 2018, the Court REPORTS and RECOMMENDS the Motion to Suppress be DENIED. I. FACTS Recitation of allegations in the superseding indictment and search warrant affidavit in no way implies adoption of them, but instead merely provides helpful context for discussion of the challenged search warrant. A. The Superseding Indictment Allegations The superseding indictment alleges the following facts. On January 11, 2013, May 1, 2013, March 25, 2015, and April 15, 2015, Mr. Roper, as a present official of the United States government, knowingly disclosed contract bid and proposal information and source selection information before the award of a federal procurement contract. (Doc. no. 83, ¶¶ 1- 4.) influenced in the performance of his official acts and \$15,000.00, respectively. (Id. ¶ 6.) On February 11, 2013, January 16, 2014, and

January 27, 2015, Mr. Roper filed financial disclosure reports falsely stating he had not received income and gifts from prohibited sources during the reporting period. (Id. ¶¶ 8-10.) On December 15, 2015, Mrs. Roper falsely stated to federal law enforcement agents she had never heard of Quadar Group and was unaware Mr. Roper received payments from Communications, Research, Engineering, and Consultants Group, LLC (Id. ¶ 11.) From December 2015 through November 2016, Defendants made false statements

the bribery, procurement integrity fraud violations, and other corrupt dealings . Id. ¶¶ 7, 13.) B. The Comcast Warrant and Supporting Affidavit



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

On January 13, 2016, U.S. Army Criminal Investigation Command Special Agent Preston T. Johnson obtained a search warrant for Comcast email account quadar@comcast.net. (For the Record 10:12:30 10:12:47.) SA Johnson alleged the following facts in his supporting affidavit.

Mr. Roper was a colonel in the U.S. Army and the Director of the Training and , Capability Manager, Network & Servic the award of sole-source contracts to CREC Group. (Doc. no.

50-2, p. 4.) Calvin Lawyer, a retired U.S. Army colonel, founded CREC in 2006 while he was serving in the U.S. Army as the TCM N&S. (Id. at 5.) CREC began working on federal contracts as a subcontractor after Mr. Lawyer retired from the U.S. Army in 2008. (Id.) Mr. Roper was responsible for approving CREC invoices during 2008 and 2009. (Id.) CREC paid Mr. Roper \$24,400.99 in 2008 and \$48,315.20 in 2009. (Id.) In paperwork submitted to the Small Business Administration, CREC stated the Quadar Group payments were for (Id.) Mrs. Roper is the (Id. at 6.)

In 2010 and 2011, while deployed in Kuwait to oversee communications infrastructure projects, Mr. Roper arranged for CREC to perform work as a subcontractor for Raytheon NIS. In those same two years, CREC paid Mr. Roper \$43,000. (Id.) In 2012, upon his return to Fort Gordon as director of TCM N&S, Mr. Roper signed a justification that resulted in the award of sole-source contracts to CREC in excess of \$20 million. (Id.) From 2008 through 2014, CREC paid Mr. Roper at least \$199,278. (Id.)

Mr. Roper utilized his military email account to communicate with Mr. Lawyer from 2009 through 2014. (Id. at 8.) On many occasions, Mr. Roper emailed sensitive government procurement information from his military account to his Comcast account, including (1) performance work statements; (2) independent government cost estimates; (3) specifications for an upcoming information technology purchase; (4) labor rate tables from existing contracts; and (5) job descriptions under existing contracts. (Id. at 9.)

Attachment A to the warrant described the property to be produced by Comcast as (Id. at 3.) Attachment B(I) more specifically ordered Comcast to produce (1) emails and attachments associated with the account; (2) information regarding identification of the account user; (3) information regarding the types of services utilized by the user; (4) information stored in the account such as address books, calendar data, and pictures; and (5) communications between Comcast and any person regarding the account. (Id. at 4-5.) Attachment B(II) to the warrant limited the Comcast production to the following categories:

All information described above in Section I that constitutes evidence and of [sic] violations of 18 U.S.C. § 201 (Bribery), 18 U.S.C. § 201(c) (Gratuities) and 18 U.S.C. § 371 (Conspiracy), among others, those violations involving COL Anthony T. ROPER and occurring after 1 June 2008, including . . . information pertaining to the following matters:

(a) Evidence of unauthorized communications involving Government



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

procurement information. (b) Evidence of conversations between COL ROPER and Mr. Calvin

LAWYER. (c) Evidence of conversations between COL ROPER and anyone else

that conveys knowledge of conflicts of interest, bribery, kickback scheme, or Procurement Integrity Act violations. (d) Evidence indicating how and when the email account was accessed

or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner; (e) relates to the crime under investigation; (f) The identity of the person(s) who created or used the user ID,

including records that help reveal the whereabouts of such person(s). (g) The identity of the person(s) who communicated with the user ID

about matters relating to Government procurement and/or COL

(Id. at 6-7.)

C. Special Agent Review of Comcast Production and Seizure of

Information Comcast saved the production to three folders on a disc and delivered it on January 29, 2016. (FTR 10:13:32 10:13:45.) SA Johnson saved the three production folders onto the hard drive of his work laptop computer for review. (FTR 10:13:50 10:14:02.) SA Johnson testified the production was voluminous, although he had no idea whether the 15 10:20:50.) He described a large but unspecified number of emails in the production as advertisements or spam. (FTR 10:26:50 10:27:02.) Over a period of approximately two weeks, SA Johnson reviewed the production and transferred to separate folders on his hard drive thirty-four or thirty-five emails he determined fell within the scope of seizure authorized by Attachment B(II). (FTR 10:14:10 10:14:45.) SA Johnson testified he never removed the three folders containing the entire production from his hard drive and still maintains the production there. (FTR 10:17:08 10:17:15.) While SA Johnson has mainly worked within the small folders containing the relevant emails, he did access the larger folders containing the entire production in preparation for the suppression hearing. (FTR 10:27:32 10:27:50.) SA Johnson has not made a the larger production folders since his initial review. (FTR 10:27:58 10:28:20.) II.

DISCUSSION Defendants argue the email production should be suppressed because (1) the warrant violated the Fourth Amendment particularity requirement by authorizing production of the entire email account rather than a limited production of emails relevant to the investigation; and (2) SA Johnson exceeded the scope of his seizure authority under Attachment B(II) by maintaining the entire production on his hard drive after the initial review. As explained below, the warrant is sufficiently particular, and while SA Johnson did exceed the scope of his seizure authority, his good faith compliance efforts render suppression of the production unjustifiable. The Court thus recommends denial of the suppression motion.



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

A. The Comcast Warrant Does Not Violate the Fourth Amendment

Particularity Requirement. The Fourth Amendme United States v. Wuagneux, 683 F.2d 1343, 1348

(11th Cir. 1982) (citations omitted). A warrant that fails sufficiently to particularize the place or things to be seized is unconstitutionally overbroad, and the resulting search is unconstitutional. United States v. Travers, 233 F.3d 1327, 1329-30 (11th Cir. 2000); United States v. Mitchell 751, 754 (11th Cir. 2013). A description is sufficiently particular when it enables the searcher reasonably to ascertain and identify the things to be seized. United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011). Technical perfection in the description is not required, but rather the Court should apply a practical margin of flexibility. Id.

Federal courts routinely uphold warrants requiring production of all information associated with a computer hard drive or email account in the face of challenges based on the particularity requirement, so long as the warrant limits seizure to relevant evidence. See United States v. Richards, 659 F.3d 527, 539 (6th Cir. 2011) (collecting cases upholding warrants authorizing seizure and search of entire personal or business computers); United States v. Lee, No. 1:14-cr-227-TCB-2, 2015 WL 5667102, *3-4 (N.D. Ga. Sept. 25, 2015) entire contents of an email account and then describes a subset of that information that will

; United States v. Intakanok, No. CR 114-060, 2014 WL 4825368, *7-8 (S.D. Ga. Sept. 25, 2014) ; In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014) (collecting federal cases upholding warrants requiring . Thus, the Court finds the Comcast warrant is sufficiently particular to satisfy the Fourth Amendment. Defendant argues the Eleventh Circuit recently rejected this precedent in United States v. Blake, 868 F.3d 960, 974 (11th Cir. 2017), cert. denied sub nom Moore v. United States, 138 S. Ct. 753 (2018). A careful reading of the decision proves otherwise. In Blake, the defendants were running a prostitution ring and posted advertisements for prostitution services on the website Backpage. Id. at 966. The FBI obtained a search warrant for Microsoft to produce from two email accounts Id. For example, the warrant required

Microsoft to turn over all emails related to Backpage.com or other online adult service websites. Id. The FBI also obtained warrants for two Facebook accounts, requiring Facebook to disclose emporal limitations. Id. However, the government Id. at 967.

The defendants argued the warrants did not satisfy the Fourth Amendment particularity requirement. Id. at 973. The court held the Microsoft warrant complied with the particularity requirement, despite the absence of any temporal limitations, because it limited disclosure to discrete categories of emails connected to the alleged crime. Id. at 973 n.7. The court commented the Facebook warrants from inception of the accounts, including every private message, photograph,



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

private or public group, Facebook search, marketplace purchase, and contact list. Id. at 966- 67, 974. While never holding the Facebook warrants violated the particularity requirement, the court commented the govern reasonable limitations concerning the time period and/or topical scope of the warrants. In support, the court pointed to published Facebook guidelines for law enforcement showing that, o Facebook account searches, the government need only send a request Id. at 974. Despite these concerns, the court declined to decide whether the Facebook warrants satisfied the particularity requirement and instead relied on the Leon [468 U.S. 897 (1984)] good faith exception to uphold the warrants. Id. There are at least three reasons Blake does not require a finding the Comcast warrant violates the particularity requirement of the Fourth Amendment despite the absence of topical and temporal limitations. First, enforcement handbook suggests it is willing to conduct searches and respond, as the Blake

policy, Law Enforcement Handbook, Comcast Cable, <http://xfn.tv/2ojXqXH> (last visited Feb. 29, 2018). Absent any indication of such extraordinary cooperation and effort by Comcast, limiting the production to key words or topics would be unworkable and a waste of time. Second, investigating white collar schemes is normally far more complex than prostitution, which makes limitations by topic or key words far more difficult. This is no less true today than when the Eleventh Circuit explained as much in its seminal Wuagneux decision:

[E]ffective investigation of complex white-collar crimes may require the pieces of individual evidence Accordingly, in cases . . . involving complex financial transactions and widespread allegations of various types of fraud, reading the warrant with practical flexibility entails an awareness of the

Wuagneux, 683 F.2d at 1349 (citations omitted). Unlike the prostitution ring at issue in Blake criminal activity includes fraud, bribery, and financial transactions related to government contracts for information technology services. Because the activity is significantly more complex than a prostitution ring, the Court may justifiably read the warrant with greater practical flexibility. Id.

Third, the Blake court endorsed limiting email and Facebook warrants of time during which [the defendant] was suspected of taking part in the prostitution Blake, 868 F.3d at 974. Here, the affidavit established probable cause to believe Defendants formed Quadar Group for the sole purpose of furthering the conspiracy. The name of the email account, quadar@comcast.net, by itself established probable cause to believe Defendants created the account to conduct Quadar Group business in furtherance of the conspiracy, such that emails from inception of the account forward would likely be relevant to the investigation.

A warrant seeking emails from the inception of an account created to further a criminal scheme is reasonable and consistent with the particularity requirement of the Fourth Amendment. That Mr. Roper might have also used the email account for personal correspondence unrelated to Quadar Group does not render the warrant unconstitutional. See *United States v. Matter of Search of Information Associated With Fifteen Email Addresses Stored at Premises Owned, No.*



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

2:17-CM-3152-WC, 2017 WL 4322826, *8 (M.D. Ala. Sept. endants chose to use the same email accounts for personal communications that they were simultaneously using to conduct their allegedly fraudulent business cannot insulate those email accounts from a search pursuant to the all records

For all of the above reasons, the Comcast warrant does not violate the Fourth

B. Even in the Event of a Constitutional Infirmary, the Leon Good Faith

Exception Applies. The Leon good faith exception saves the warrant from any constitutional deficiency that may exist. The judicially created remedy known as the exclusionary rule acts as a deterrent to violating the Fourth Amendment by preventing the use of evidence seized as a result of an illegal search. *United States v. Leon*, 468 U.S. 897 (1984); *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002). However, under Leon, the good faith exception all

Leon, 468 U.S. at 913. The Leon Court explained that the good faith exception to *Id.* at 916.

Thus, under Leon, the question becomes whether the officers executing the warrant See *id.* at 913; see also *United States v. Herring* exclusionary rule does not bar the use of evidence obtained by officers acting in good faith

Under Leon, there are four scenarios under which the good faith exception to the exclusionary rule would not apply. The exception does not apply where the judge issuing the warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth. *Leon*, 468 U.S. at 923. Nor does the exception apply in cases detached and neutral judicial role such that no reasonably well-trained officer would rely on the warrant. *Id.* probable cause as presume it was valid. *Id.*

Here, there is no suggestion or evidence false information was provided or the issuing

And the parties do not dispute the warrant applications established probable cause. Additionally, the warrants are not so facially deficient in any respect that the executing officers could not reasonably presume them to be valid. In *Blake*, even though the Facebook warrants at that could be found in a social media

the court held it was not so facially deficient that the executing officers could not have reasonably believed it to be valid. *Id.* The same is true here.

C. Special Agent Johnson Improperly Executed the Comcast Warrant but

Suppression Is Not Justified. Defendants argue SA Johnson exceeded the scope of his seizure



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

authority under the warrant by keeping the entire production saved on his laptop after moving relevant emails to separate folders, rather than deleting the production folders and keeping only the original production disc. (Doc. no. 82, pp. 3-6.) The government argues SA Johnson sufficiently distinguished between the items he seized and those he did not by segregating them in folders on his laptop. (Doc. no. 56, pp. 7-8.)

United States v. Ramirez, 523

U.S. 65, 71 (1998) (internal citation omitted). e manner in which a warrant is executed Dalia v. United States, 441 U.S. 238, 258 (1979) (citation omitted). public interest and the in Pennsylvania v. Mimms, 434 U.S. 106, 109 (1977) (quoting United States

v. Brignoni-Ponce of the facts of cases so various that no template is likely to produce sounder results than

United States v. Banks, 540 U.S. 31, 36 (2003). The Court sees no meaningful distinction between SA initial production and the segregated emails, and thus no basis for finding he seized the

emails saved in the relevance folders but did not seize the original production saved in separate yet equally accessible folders. By retaining the complete original production on his laptop hard drive for more than two years after completing his review, SA Johnson seized all of the data disclosed by Comcast, including data the warrant did not authorize to be seized. SA Johnson thus exceeded the scope of the warrant in violation of the Fourth Amendment.

Although SA Johnson exceeded the scope of the warrant, blanket suppression is not United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007) (citation

outside the scope of a warrant will not affect admissibility of items properly seized, or

constitu Id. (citations omitted).

SA contrary, he attempted to honor its restrictions by segregating the subset of relevant emails

into separate folders, limiting his subsequent work to those folders, and accessing the original production folders only once thereafter, as he recalled, to verify information in preparation for the suppression hearing. (FTR 10:27:32 10:27:50.) Just as importantly, the warrant did not specify what actions should be taken to limit access to the original production once the initial review for relevant emails was complete. (Doc. no. 50-2.) Even Defendants concede the government had to retain the original Comcast production on the disc to produce discovery to them. (FTR 10:51:52 10:53:23.) Accordingly, suppression is not warranted, and SA the relevant emails he seized.



USA v. Roper et al

2018 | Cited 0 times | S.D. Georgia | March 1, 2018

To remedy the warrant violation, the Court recommends inclusion of a directive in the final order requiring SA Johnson, with issuance, to (1) designate an IT expert from the U.S. Army Criminal Investigation Command to remove the Comcast production from SA Johnson's laptop computer, except for the small subset of approximately thirty-five emails SA Johnson previously determined to be relevant; and (2) submit an affidavit executed by SA Johnson and the IT expert confirming compliance with this directive. III. CONCLUSION

For the reasons set forth above, the Court REPORTS and RECOMMENDS Defendants Motion to Suppress (doc. no. 50) be DENIED and SA Johnson be ORDERED to remove the original production from his laptop computer in the manner described above.

SO REPORTED and RECOMMENDED this 1st day of March, 2018, at Augusta, Georgia.

