IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALBERT DEWAYNE BANKS et al.

Defendant.

Case No. 5:13-cr-40060-DDC

MEMORANDUM AND ORDER

Defendants Taylor, Thompson, and Makdins have filed motions to suppress intercepted text messages, and other defendants have joined their motions (Doc. 351, 356, 375). Defendants argue, among other things, that the Court must suppress text message evidence because investigators intercepted them pursuant to orders, which, on their face, authorized interception of wire communications only. For the reasons set forth below, the Court denies defendants' motions to suppress text message evidence on this basis.

Background

Investigators obtained wiretap orders in the final months of a thirteen-month investigation into a suspected narcotics-trafficking conspiracy. The investigation was a joint effort by the Kansas Bureau of Investigation ("KBI"), the Junction City Police Department, the Geary County Sherriff's office, and the Riley County Police Department. Beginning in March of 2013, investigators submitted applications for wiretap orders to Judge Platt, a judge in Kansas' Eighth Judicial District. Judge Platt issued a total of eight wiretap orders under the authorization

granted by the Kansas wiretap statute, K.S.A. § 22-2514 *et seq*. The dates of issuance and expiration of each of the orders are set forth below:

- Thompson Order #1 (1783) Issued March 5; Expired April 4.¹
- Banks Order #1 (6704) Issued March 5; Expired April 4.²
- Ivory Order #1 (7176) Issued April 2; Expired May 2.³
- Ponds Order #1 (0088) Issued April 2; Expired May 2.⁴
- Thompson Order #2 (1783) Issued April 4; Expired May 4.⁵
- Ivory Order #2 (7015) Issued April 12; Expired May 12.⁶
- Banks Order #2 (9771) Issued April 12; Expired May 12.⁷
- Thompson Order #3 (2893) Issued April 16; Expired May 16.⁸

Each order provided authorized interception of "wire communications." See, e.g., Doc. 379-1 at

3. No orders authorized interception of "electronic communications." Nonetheless, investigators believed that the orders permitted the interception of text messages, and service providers in fact intercepted text messages sent to and from the target phones throughout the duration of each wiretap order.

- ¹ Doc. 379-1.
- ² Doc. 379-2.
- ³ Doc. 379-3.
- ⁴ Doc. 379-5.
- ⁵ Doc. 379-7.
- ⁶ Doc. 379-11.
- ⁷ Doc. 379-13.
- ⁸ Doc. 379-15.

Analysis

A. Governing Law

"Title III of the Omnibus Crime Control and Safe Streets Act, codified in 18 U.S.C. § 2510 *et seq.*, which preempts the field of electronic surveillance regulation, allows for concurrent state regulation, subject, at the minimum, to the federal regulatory requirements" *State v. Willis*, 643 P.2d 1112, 1114 (Kan. Ct. App. 1982). "Although a state may adopt a wiretap statue with standards more stringent than the federal requirements, a state may not adopt more permissive standards." *Id.* "Accordingly, where there are at issue provisions of a state wiretap statute which conform to their counterparts in the federal act, federal case authority has precedential value at least equivalent to state case authority, if any. Hence, federal case law in this area is generally, if not universally, treated as controlling authority." *Id.* The Court finds that K.S.A. § 22-2516 and 18 U.S.C. § 2518(8)(a) are identical with respect to the issues the motions raise.

Both statutes govern interception of "wire, oral, and electronic communications." *See* K.S.A § 22-2514(1) *et seq*; 18 U.S.C. § 2510 *et seq*. Defendants rightly point out that the statutes distinguish between wire and oral communications: "'wire communication' refers "to any aural transfer" K.S.A § 22-2514(1); 18 U.S.C. § 2510. In contrast, "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature . . . but does not include: [a]ny wire or oral communication;" K.S.A § 22-2514(11); 18 U.S.C. § 2510(12). Defendants are also correct that text messages constitute "electronic communication" and not "wire communication" because they involve no "aural transfer." *See United States v. Jones*, 451 F. Supp. 2d 71, 75 (D.D.C. 2006) (text messages constitute "electronic communications"). Significantly, the statutory suppression

remedy in both the Kansas wiretap statute and Title III apply to wire and oral communications only.

Any aggrieved person in any trial, hearing or proceeding in or before any court, department, officer, agency, regulatory body or other authority of the United States, this state, or a political subdivision thereof, may move to suppress the contents of any intercepted *wire or oral communication*, or evidence derived therefrom, on the grounds that: . . . (iii) the interception was not made in conformity with the order of authorization.

K.S.A. § 22-2516(9)(a) (emphasis added); 18 U.S.C. § 2518(8)(a) (same).

The statutes do mandate suppression of intercepted electronic communication for certain violations. *See*, *e.g.*, K.S.A. § 22-2516(8)(a) (failure to seal recordings of intercepted wire, oral, or electronic communications immediately requires suppression of such evidence). But where the alleged violation is that "the interception was not made in conformity with the order of authorization," as defendants allege here, the statutory suppression remedy extends to wire and oral communications only. *Id.* at § 22-2516(9)(a). The omission of "electronic communications" from the suppression provision was not a mere oversight. The statute goes on to clarify that:

The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for *nonconstitutional* violations of this act involving such communications.

K.S.A. § 22-2516(12) (emphasis added); see also 18 U.S.C. § 2518(10)(c) (same).

Case law interpreting the identical Title III provisions supports this conclusion. See, e.g.,

United States v. Steiger, 318 F.3d 1039, 1051 (11th Cir. 2003) (citing United States v.

Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) ("The ECPA does not provide an independent

statutory remedy of suppression for interceptions of electronic communications); United States v.

Reyes, 922 F. Supp. 818, 837 (S.D.N.Y. 1996) (holding that exclusion of evidence is not a

remedy for the ECPA violation)). In general, "Fourth Amendment precedent is highly relevant in deciding whether an authorizing [wiretap] order is valid and whether a defect in wording is of a kind that threatens the central interests sought to be protected." *United States v. Cunningham*, 113 F.3d 289, 294 (1st Cir. 1997). Such precedent is especially relevant to this case, because the Fourth Amendment's exclusionary rule offers the only suppression remedy available for interception of electronic communications. K.S.A. § 22-2516(12); 18 U.S.C. § 2518(10)(c). Accordingly, the Court looks to Fourth Amendment precedent, including any applicable exceptions to the exclusionary rule, to determine whether Judge Platt's failure to include "electronic communications" in the wiretap order requires suppression of intercepted text messages.⁹

B. The Existence of a Constitutional Violation

Because the statutory suppression remedy does not extend to nonconstitutional violations involving electronic communications, the Court must resolve two questions: (1) whether the interception of text messages arose to a constitutional violation; and (2) if so, whether the exclusionary remedy of the Fourth Amendment applies.

⁹ The Court recognizes that Kansas constitutional law also applies to this case. However, The Kansas Supreme Court has interpreted § 15 of the Kansas Constitution Bill of Rights to provide the same protection from unlawful government searches and seizures as the Fourth Amendment does. *State v. Neighbors*, 328 P.3d 1081, 1086 (Kan. 2014). Kansas also has incorporated the good-faith exception into its constitutional law. *State v. Daniel*, 242 P.3d 1186, 1189 (Kan. 2010). The Court, therefore, relies primarily on the more developed federal cases applying the Fourth Amendment.

For a court to suppress evidence based on a violation of the Fourth Amendment, a defendant bears the burden to prove an unlawful search and that he had a legitimate expectation of privacy in the searched item. *United States v. McKennon*, 814 F.2d 1539, 1542 (11th Cir. 1987). To establish a reasonable expectation of privacy, the defendant must show that: (1) he manifested "a subjective expectation of privacy;" and (2) society recognizes that expectation as "legitimate." *Id.* at 1543. If the defendant establishes an expectation of privacy, then the burden shifts to the government to show that the search was reasonable under a recognized exception to the warrant requirement. *United States v. Harris*, 526 F.3d 1334, 1338 (11th Cir. 2008).

The Tenth Circuit has not decided whether individuals have a legitimate expectation of privacy in text messages. But other circuits have so held, *see United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007), as have several district courts. *See United States v. Davis*, 787 F. Supp. 2d 1165, 1170 (D. Or. 2011); *United States v. Morales-Ortiz*, 376 F. Supp. 2d 1131, 1140 (D.N.M. 2004). The Supreme Court has suggested, but has not held, that individuals have a reasonable expectation of privacy in text messages. *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (noting that "text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification," but declining to find a reasonable expectation of privacy a police officer's text messages stored on a department-issued cell phone). For the purposes of this analysis, the Court assumes defendants have established an expectation of privacy in their text messages, and that society recognizes their expectation as legitimate. *United States v. Reza*, 315 F. App'x 745, 747 (10th Cir. 2009) (Courts have discretion "to proceed directly to an analysis of the good-faith exception without first addressing the underlying Fourth Amendment question."). The

government therefore bears the burden to show that the search was reasonable under a recognized exception to the warrant requirement. *See Harris*, 526 F.3d at 1338.

C. The "Good-Faith" Exception

The government presented evidence that investigators intercepted text messages based on a mutual understanding with Judge Platt. This understanding, the government argues, brings investigator's conduct within the "good-faith" exception to the warrant requirement articulated in *United States v. Leon*, 468 U.S. 897 (1984). The good faith exception applies when an officer has a good faith but incorrect or mistaken belief about a fact. *United States v. Salinas–Cano*, 959 F.2d 861, 865 (10th Cir. 1992). In *Leon*, the Supreme Court held that evidence seized by police officers acting in reasonable and good-faith reliance on a search warrant that was, ultimately, unsupported by probable cause need not be suppressed. *Id.* at 922. Subsequent decisions have applied the *Leon* test to warrants that insufficiently describe the objects of a search or seizure. *See, e.g., Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984); *United States v. Cunningham*, 113 F.3d 289, 294 (1st Cir. 1997); *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986).

The Court must therefore determine whether the KBI officers' reliance on Judge Platt's wiretap orders was objectively reasonable. "A substantial body of Fourth Amendment precedent ... permits a reviewing court to consider the knowledge of the officials who approved a warrant and executed it." *Id.* The rationale for considering the personal knowledge of an executing officer is that such knowledge may show "that there was *in fact* no real threat to legitimate privacy interests." *Id.* Thus, to determine whether the good-faith exception should rescue otherwise defective wiretap orders, the Court considers the personal knowledge Judge Platt and the KBI officers had about the type of communications the order intended to authorize. *Id.*

Where the government seeks to rescue a defective warrant based on the knowledge of the issuing judge and executing officers, the government bears the burden of proving such knowledge. *Id.* at 295.

Both Judge Platt and the KBI understood the orders to authorize interception of text messages as well as oral communications. Special Agent Virden, who headed the investigation for the KBI, testified that the investigators, based on conversations with Judge Platt, understood the orders to authorize interception of text messages. Moreover, affidavits in support of subsequent wiretap applications contained evidence of text messages intercepted pursuant to previous orders, which apparently authorized interception of wire communications only. For example, the affidavit in support of Ponds Order #1 contained references to text messages intercepted pursuant to the Thompson Order #1. Doc. 379-6 at 10. There is no evidence that Judge Platt objected or acted surprised when the later affidavits revealed that agents had intercepted text messages. To the contrary, Judge Platt issued "Clarification Orders" when two wireless carriers refused to provide text messages because they did not read Ponds Order #1 and Thompson Order #2 to authorize interception of text messages. Doc. 379-9; Doc. 379-10. The Clarification Orders stated that:

[T]he interception of wire communications previously authorized includes all forms of communication set forth in K.S.A. 22-2514, to wit: oral, wire, or electronic communications to and from said telephone including the interception of "SMS data" or messaging.

The Clarification Orders only applied to Ponds Order #1 and Thompson Order #2. Special Agent Virden testified that Judge Platt clarified those two orders only because those two carriers were the only carriers who refused to intercept texts without clarification from Judge Platt and not because they were the only orders for which Judge Platt meant to authorize interception of

text messages. Although the Clarification Order only extended to two of the wiretap orders, the Court views the Clarification Orders as evidence of a broader understanding between Judge Platt and the KBI that the orders were supposed to authorize interception of electronic communications.

The Court finds that the issuing judge and executing officers both understood the intended scope of the wiretap authorization, and that the authorization included interception of text messages. The Court also finds that the officers' reliance on this understanding was "objectively reasonable." *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested."). As a result, the KBI's interception of text messages falls within the good-faith exception to the Fourth Amendment's exclusionary rule, and the Court refuses to suppress them on the basis that the orders authorized interception of wire communications only.

IT IS THEREFORE ORDERED BY THE COURT THAT the Defendants Taylor and Makdins' motions to suppress electronic communications (Docs. 351, 375) are denied. The portion of defendant Thompsons' motion (Doc. 356) that seeks suppression of electronic communication is also denied. The remaining defendants' motions are denied to the extent that they joined these motions' effort to seek suppression of the intercepted text messages.

IT IS SO ORDERED.

Dated this 29th day of August, 2014, at Topeka, Kansas.

<u>s/ Daniel D. Crabtree</u> Daniel D. Crabtree United States District Judge