

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

Case No.: 1:19-CR-00018-ABJ

UNITED STATES OF AMERICA,

v.

ROGER J. STONE, JR.,

Defendant.

DEFENDANT ROGER STONE'S MOTION TO SUPPRESS

Defendant ROGER STONE, files this motion to suppress all evidence as fruit of illegal search warrants executed on specified dates and times. The warrants and applications are filed under seal.

BACKGROUND

The Government stated in its Opposition to Stone's Motion to Dismiss (Dkt # 99) that it will not be required to prove that the Russians hacked either the Democratic National Committee ("DNC") or Democratic Congressional Campaign Committee ("DCCC") from outside their physical premises or that the Russians were responsible for delivering the data to WikiLeaks. These assumptions formed the inadequate basis for the search warrants conducted in this case and the Indictment of Defendant. In addition to the fundamental assumptions, the government designated Roger Stone's case as related to *United States v. Netyksho et. al.* No. 18-cr-215 (ABJ) and cites to this Indictment in certain search warrant applications. (*See e.g.* Exhibit, Google search warrant application at 6, ¶18). If these premises are not the foundation for probable cause, Roger Stone communicating with a Twitter user named "Guccifer 2.0" or

speaking with WikiLeaks, would not constitute criminal activity.

Roger Stone has been charged with obstruction of Congress, lying to Congress, and witness tampering under 18 U.S.C. §§ 1505, 1001, 1512(b)(1), 2. The search warrant applications however, allege that the FBI was investigating various crimes at different times, such as Stone for accessory after the fact, misprision of a felony, conspiracy, false statements, unauthorized access of a protected computer, obstruction of justice, witness tampering, wire fraud, attempt and conspiracy to commit wire fraud, and foreign contributions ban. The uncharged conduct particularly relied upon the assumptions the Russian state is responsible for hacking the DNC, DCCC,¹ and even (although not as clear) Hillary Clinton campaign manager, John Podesta.

There is a certain forensic methodology that the FBI, Secret Service, or any other law enforcement agency conducting a computer forensic analysis follows. The first, and arguably most crucial step in the evidence gathering process, is to preserve the evidence. The imaging of the forensic data in its native format is key to preserving forensic evidence so as to allow agents to present authentic evidence in Court. Federal Rule of Evidence 902(14) permits authentication through a “process of digital identification by a qualified person” as long as it complies with Rule 902(11).² That Rule requires compliance with the business records exception of hearsay: “the record was made at or near the time by – or from information transmitted by someone with knowledge.” Fed.R.Evid. 803(6)(a). Neither the Mueller report (from what we can tell), nor the CrowdStrike Reports (also heavily redacted) provide sufficient indicia of authenticity.

¹ WikiLeaks never released the DCCC documents. The Mueller report suggests the hack of the DCCC only provided additional keys to access the DNC servers. (Mueller Report at 38).

² “A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.” Fed.R.Ev.902(14) (Comm. note).

Based on the information available, the DNC either failed to alert the FBI about a major security breach of its systems, or the FBI chose not to respond to said breach. Consequently, the DNC hired a private company – CrowdStrike. It is also unclear if the FBI ever conducted a forensic analysis on the DCCC servers. It is clear, however, that the government has relied on the assumptions made by a source outside of the U.S. intelligence community that the Russian State was involved in the hacking and that the data taken from the various servers were given to WikiLeaks. The government cannot prove either since it did not participate in the investigation at the earliest stage. The government does not have the evidence, and it knew it did not have the evidence, when it applied for these search warrants. Now the government confesses: *“The Office cannot rule out that stolen documents were transferred to WikiLeaks through intermediaries who visited during the summer of 2016.”* (Mueller Report at 47).

The government cites to CrowdStrike,³ a private forensic computer firm, but not a government investigation through the FBI.⁴ CrowdStrike's draft reports were provided to the defense, but not finalized reports, and they were heavily redacted. The first step in any computer fraud case is to encase and image the "attacked" computer. (Exhibit, DOJ Digital Forensic Analysis Methodology). CrowdStrike failed to encase the subject computers. This failure was fatal to any effort undertaken to ensure that investigation about whether the Russian government hacked the DNC, DCCC, or Podesta's computers was competent, thorough, and done by the

³ CrowdStrike is not a government agency. It did not conduct its investigation at the behest of the government. The DNC and DCCC hired CrowdStrike to investigate the alleged theft of its data from its servers. (Indictment, ¶¶ 1-3). The CrowdStrike draft reports do not support its conclusions with evidence. In short, if this were an elementary school math problem, CrowdStrike not only does not show its work, it does not show the question – only its answer. Stone separately files a motion to compel an unredacted portion of the draft reports and any final reports. Stone also provides the draft reports of CrowdStrike under seal as Exhibits.

⁴ CrowdStrike's three draft reports are dated August 8 and August 24, 2016. The Mueller Report states Unit 26165 officers also hacked into a DNC account hosted on a cloud-computing service on September 20, 2016, thereby illustrating the government's reliance on CrowdStrike even though the DNC suffered another attack under CrowdStrike's watch. (See Mueller Report at 49-50).

book. In fact, during Roger Stone's testimony to the House Permanent Select Committee on Intelligence, a squabble between members of Congress erupted over whether and when the FBI possessed the DNC's servers. (Exhibit, Tr. at 110-112).

Attached to this motion, as exhibits, are declarations from William Binney and Peter Clay. Both concur that in their opinions, WikiLeaks did not receive the stolen data from the Russian government. Their study and examination of the intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were delivered in a medium such as a thumbdrive. The data further indicates that the files were physically and manually acquired from the DNC inside the DNC office.

The *raison d'etre* of the Special Counsel's investigation was to pursue the claims that the Russians hacked and delivered the stolen data to WikiLeaks. (See Order appointing Special Counsel, Dkt. # 69-4). The foundation of all the search warrants was similar. If that foundation collapses, then the warrants must fail for lack of probable cause. Roger Stone requests this Court grant a *Franks* hearing for the reasons stated. The Court has already set aside June 21, 2019 for hearing time to discuss anticipated motions to suppress. Stone expressly requests an evidentiary hearing at that time. If the Court were to remove from the warrant applications, all the allegations that were speculation and are unproven or unprovable, then there would be no probable cause to support a search warrant for Roger Stone's papers, emails, cell phones, computers, and other devices.

MEMORANDUM OF LAW

Roger Stone is challenging the main underpinning of the search warrant applications supporting the warrants – the Russian government hacked the DNC, DCCC, and one Clinton Campaign official from locations outside where the computer servers were stored. *First*, Stone

will demonstrate that the Government's proposition is untrue. This assumption was not based upon a government investigation disclosed to the defense; rather, it was based upon CrowdStrike's, private investigation, of the respective servers of another private organization. *Second*, it appears those servers have not been encased and consequently, its data not properly preserved. The proper preservation is critical in order for it to be admissible at trial. Because of the failure of the Government to present proof in the search warrant applications, if the Court were to remove the misrepresentation from the warrant applications, no probable cause would exist to support the search warrants themselves. Stone is entitled to an evidentiary hearing to support his case, pursuant to *Franks v. Delaware*, 438 U.S. 154, 156, 98 S. Ct. 2674, 2676 (1978).

The Fourth Amendment provides in relevant part that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." *E.g. Collins v. Virginia*, 138 S. Ct. 1663, 1669 (2018). The Fourth Amendment requires a warrant supported by probable cause in order to support a lawful search. *Id.* Because there was a search warrant application drafted by government agents based upon the underlying assumption that the Russian state hacked the DNC, DCCC, and John Podesta's emails from the outside, the fruits of the search must be suppressed. *See, e.g., Wong Sun v. United States*, 371 U.S. 471, 484 (1963).

Franks requires the Court to evaluate: 1) was there a misrepresentation in the search warrant application; 2) was the misrepresentation reckless or worse; and, 3) if it there were misrepresentations, does the application for the warrant survive without the offending misrepresentations.

We reverse, and we hold that, where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or

with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Franks, 438 U.S. at 155-56. *See also Pierce v. Mattis*, 256 F.Supp3d 7, 14 (D.D.C. 2017) (Berman Jackson, J.).

The allegations in the warrant applications are nothing more than a collection of conclusory statements. There is no evidence, only supposition. This is not a substitute for factual allegations supporting probable cause.

An affidavit in support of a warrant application “must provide the magistrate with a substantial basis for determining the existence of probable cause,” and it cannot consist of “wholly conclusory statement[s].” *Illinois v. Gates*, 462 U.S. 213, 239, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983).

“[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Id.* at 232, 103 S.Ct. 2317. The Supreme Court has recognized that the “task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information, there is a fair probability that ... evidence of a crime will be found in a particular place.” *Id.* at 238, 103 S. Ct. 2317 (abandoning the rigid two-prong test for determining informant veracity in favor of a totality of circumstances approach). Thus, a magistrate is supposed to consider the “totality-of-the-circumstances” in making probable cause determinations. *Id.*

United States v. Manafort, 313 F.Supp.3d 213, 228-29 (D.D.C. 2018). "Although we pay 'great deference' to the judge's initial determination of probable cause, a warrant application cannot rely merely on 'conclusory statement[s].'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (citations omitted). If this Court were to remove the language regarding the Russians hacking the DNC, DCCC, and Podesta, then the warrants lack probable cause. *See Franks*, 438 U.S. at 156 (removing offending portion of warrant and then evaluate probable cause); *United States v. Karo*, 468 U.S. 705, 719 (1984). If this Court were to remove the conclusory representations that the Russian state transferred the electronic data to WikiLeaks, there would be no probable cause to support the warrants. *See id.*

The indictment of Roger Stone is for obstruction of Congress, lying to Congress, and witness tampering; however, the purported crimes investigated and presented to the various courts reviewing the assorted warrants were much broader and were searching for a conspiracy between Stone, the Russians, or WikiLeaks. Because the two declarations provided to the Court debunks the underpinning of the warrants, Stone should be granted an evidentiary hearing. The government's agents knew that they could not prove the Russian state hacked the DNC or the other targeted servers, and transferred the data to WikiLeaks when it presented the search warrants to the various magistrates and district court judges.

CONCLUSION

This motion to suppress justifies an evidentiary hearing to which the Court has already set aside hearing time on June 21, 2019.

Respectfully submitted,

By: /s/ _____

L. PETER FARKAS
HALLORAN FARKAS & KITTLA, LLP
DDC Bar No.: 99673
1101 30th Street, NW
Suite 500
Washington, DC 20007
Telephone: (202) 559-1700
Fax: (202) 257-2019
pf@hfk.law

ROBERT C. BUSCHEL
BUSCHEL GIBBONS, P.A.
D.D.C. Bar No. FL0039
One Financial Plaza, Suite 1300
100 S.E. Third Avenue
Fort Lauderdale, FL 33394
Telephone: (954) 530-5301
Fax: (954) 320-6932
Buschel@BGLaw-pa.com

BRUCE S. ROGOW
FL Bar No.: 067999
TARA A. CAMPION
FL Bar: 90944
BRUCE S. ROGOW, P.A.
100 N.E. Third Avenue, Ste. 1000
Fort Lauderdale, FL 33301
Telephone: (954) 767-8909
Fax: (954) 764-1530
brogow@rogowlaw.com
tcampion@rogowlaw.com
Admitted pro hac vice

GRANT J. SMITH
STRATEGYSMITH, PA
D.D.C. Bar No.: FL0036
FL Bar No.: 935212
401 East Las Olas Boulevard
Suite 130-120
Fort Lauderdale, FL 33301
Telephone: (954) 328-9064
gsmith@strategysmith.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on May 10, 2019, I electronically filed the foregoing with the Clerk of Court using CM/ECF. I also certify that the foregoing is being served this day on all counsel of record or pro se parties, via transmission of Notices of Electronic Filing generated by CM/ECF.

BUSCHEL GIBBONS, P.A.

_____/s/ Robert Buschel_____
Robert C. Buschel

*United States Attorney's Office for the
District of Columbia*

Jessie K. Liu
United States Attorney
Jonathan Kravis
Michael J. Marando
Assistant United States Attorneys
Adam C. Jed
Aaron S.J. Zalinsky
Special Assistant United States Attorneys
555 Fourth Street, NW
Washington, DC 20530
Telephone: (202) 252-6886
Fax: (202) 651-3393