

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES OF AMERICA	)	
	)	
V.	)	Crim. No. 15-cr-10271-WGY
	)	
ALEX LEVIN	)	<b><u>FILED UNDER SEAL</u></b>
_____	)	

**DEFENDANT’S MOTION TO SUPPRESS EVIDENCE**

The defendant, Alex Levin, moves this Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) to suppress all evidence obtained from the Government’s illegal search of his computer through the deployment of a “Network Investigative Technique,” in violation of 28 U.S.C. § 636(a) and Fed. R. Crim. P. 41. This includes all evidence, including computers and digital images, seized from the defendant on August 12, 2015 pursuant to a search warrant based on information derived from an earlier unlawful search.

**STATEMENT OF FACTS**

On August 12, 2015, FBI agents executed a search warrant at the home of the defendant, Alex Levin, in Norwood, Massachusetts. The search was conducted pursuant to Search Warrant #15-MJ-2187, issued by Magistrate Judge Marianne B. Bowler of the District of Massachusetts on August 11, 2015. The warrant application was based upon the affidavit of Detective Michael Sullivan of the Boston Police Department, who was a

member of the FBI Child Exploitation Task Force. The search warrant and affidavit are attached hereto as Exhibit 1 (hereinafter "the Residential Warrant").

The affidavit in support of the Residential Warrant primarily relied upon information derived from an investigation into a Website referred to in the affidavit as "Website A." See Exh. 1 at ¶ 9. The affiant described Website A as "a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." *Id.* Government investigators seized the computer server hosting Website A in North Carolina on February 20, 2015, and brought it to Virginia. *Id.* The FBI assumed administrative control over the website and continued to operate it from a government facility in Virginia.<sup>1</sup> See Application for an Order Authorizing Interception of Electronic Communications, dated February 20, 2015, at ¶ 52 (hereinafter, the "Title III Order")(attached hereto as Exhibit 2). The website was in operation until March 4, 2015. Exh. 1 at ¶ 9. It is apparent

---

<sup>1</sup> The affidavit in support of the Residential Warrant states only that "[t]he website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time 'Website A' ceased to operate." Exh. 1 at ¶ 9. The affidavit does not mention that it was, in fact, the FBI itself who was operating the website during this thirteen-day period.

that during this time, the FBI was making child pornography available for download to an unknown number of potential users.

Investigators discovered that the website encouraged users to register anonymously using a false email address. *Id.* at ¶ 10-12. After registering, users could then access different sections of the website, including forums and sub-forums relating to sexual exploitation of children. *Id.* at ¶ 13. According to the affidavit in support of the Residential Warrant, a majority of these forums contained images of child pornography and child erotica. *Id.* at ¶ 16. The website also allowed users to upload child pornography and included discussion boards relating to the perpetration of child sexual abuse. *Id.* at ¶ 18, 19.

On February 20, 2015, the same day it seized the server, the government obtained a Title III search warrant (Exhibit 2) from a District Court Judge in the United States District Court for the Eastern District of Virginia. Exh. 1 at ¶ 9; Exh. 2. The order permitted investigators to intercept electronic communications on the site's private chat and messaging services between unknown "target subjects" or "unidentified administrators and users." Exh. 2 at ¶ 3.

Website A utilized network software that concealed users' true Internet Protocol address ("IP address"). Exh. 1 at ¶ 7-8, 21. Specifically, the website operated on an anonymous network

known as "The Onion Router" or "TOR" which prevented law enforcement from obtaining the a user's IP address without the use of a "Network Investigative Technique." ("NIT"). See Affidavit in Support of Application for Search Warrant dated February 20, 2015 at ¶ 7. (hereinafter, the "NIT warrant") (attached as Exhibit 3). Because Website A utilized the TOR network, logs of member activity contained on the seized server could not be used to locate and identify users. Exh 2. at ¶ 39.

Simultaneously with obtaining the Title III order, the Government obtained a search warrant (Exh. 3) authorizing the deployment of a Network Investigative Technique (NIT). This search warrant was issued by a Magistrate Judge of the Eastern District of Virginia. The NIT would "send one or more communications" to Website A's users that would cause the receiving computers to deliver data identifying the computer and its user to the government-controlled server in Virginia. Exh. 1 at ¶ 22; Exh. 2 at ¶ 53. This data included a broad range of information about the user's computer.<sup>2</sup>

---

<sup>2</sup> This data includes the computer's actual IP address; the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered; the computer's Host Name; the computer's active operating system username; and the computer's MAC address. Exh. 1 at ¶ 22.

The Government states that during the time it operated Website A, a user of the site named "Manakaralupa" accessed posts on the site that contained links to illegal images. *Id.* at ¶¶ 24, 25, 26. On February 23, 2015, the FBI deployed an NIT to a computer believed to be connected with "Manakaralupa" and extracted its IP address. *Id.* at ¶ 27. The NIT also provided investigators with the host and log-on names for the computer, alleged to be "Alex-PC" and "Alex." *Id.* at ¶ 28. Investigators used this information to issue an administrative subpoena to Verizon for information related to the "Manakaralupa" IP address that had been seized through use of the NIT. *Id.* at ¶ 27, 29. Verizon identified the defendant as the subscriber for the IP address. Exh. 1 at ¶ 29.

Investigators obtained the defendant's home address and applied for a search warrant. *Id.* at ¶ 30-34. The Court issued the Residential Warrant on August 11, 2015. Investigators executed the warrant the next day at his home. Agents arrested him and seized his personal computers and other digital devices which allegedly contain child pornography. The defendant is charged with one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2).

#### **ARGUMENT**

The Government's search of the defendant's computer, along with those of individuals across the country, was in violation

of the jurisdictional requirement for searches under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). This requirement authorizes a magistrate judge to issue a search warrant *only* for a location within the judicial district itself, with minor exceptions not applicable to the present scenario. This restriction is not a ministerial technicality. Rather, Rule 41 and § 636(a) serve as a critical line of protection against the nationwide searches that occurred in this case. Suppression of the seized evidence is mandated because a search warrant that the magistrate judge was not permitted by rule and statute to issue is "no warrant at all," *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring), and is "per se harmful," i.e., prejudicial, to the defendant. *See id.* at 1122.

#### **A. The Warrant Violated Rule 41**

The searches of the defendant's home and computer devices on August 12, 2015 were the direct result of the illegal search of his computer—and countless others<sup>3</sup>—through the use of an NIT. The NIT Warrant issued by a magistrate judge of the Eastern District of Virginia violated the clearly established jurisdictional limits set forth in Fed. R. Crim. P. 41. It allowed government agents to conduct a borderless dragnet search

---

<sup>3</sup> See Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, January 5, 2015, available at: <http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers>.

with no geographic limitation. Rule 41 simply does not permit a magistrate judge in Virginia to authorize the search of the defendant's computer located in Massachusetts.

Rule 41(b) provides a magistrate judge with authority to issue a warrant in five unambiguous circumstances:

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property *located within the district*;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property *outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed*;

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant *to install within the district a tracking device*; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, *but within any of the following*:

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

(emphasis added). The warrant in this case is not authorized under any of these sections and is therefore plainly unlawful.

**1. The Warrant is Not Authorized Under Rule 41(b)(1).**

Rule 41(b)(1) allows a magistrate judge to issue a warrant for people or property located within that judge's district. The NIT Warrant inaccurately states that the evidence sought is "located in the Eastern District of Virginia." Attachment A to the NIT Warrant indicates that the computer server, located in Virginia, is the place to be searched. Exh. 3, Attachment A. Yet the server for the "Target Website" was already under FBI control in the district. The actual "place to be searched" was the myriad of "activating computers – wherever located" that would unknowingly download the NIT, thereby forcing the transmission of their internal data back to the FBI in Virginia. See Exh. 3 at ¶ 46. The NIT Warrant authorized these searches even though there was no basis from which to conclude that these computers would be located in the Eastern District of Virginia.

Rule 41(b)(1) cannot be the basis for the search of the defendant's computer in Massachusetts.

Lest there be any doubt about whether it was the defendant's computer that was searched rather than the Virginia server, the Government explained the need for the NIT on the basis that possession of the server alone would not allow the Government to identify the site's users. Exh. 2 at ¶ 58. In order to do so, it was necessary to deploy the NIT so that the defendant's computer would download the NIT and allow the Government to seize this information in Massachusetts before sending it to Virginia. Thus, although the NIT was first deployed from the server in Virginia, it is clear that the actual search occurred when the NIT was installed on the defendant's computer and extracted its data. This situation is no different from agents claiming that a search took place in Virginia because they traveled to Massachusetts, copied data from a computer, and returned to Virginia before examining the contents. The fact that the Government is now capable of seizing data on a computer without physically traveling to its location does not alter this analysis.

In a similar case, *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. 2016), the court found the argument that the crimes were committed "'within' the location of Website A, Eastern District of Virginia, rather than on the personal computers

located in other places under circumstances where users may have deliberately concealed their locations" to be "unpersuasive." 2016 WL 337263 at \*6. As is the case here, "because the object of the search and seizure was [the defendant's] computer, not located in the Eastern District of Virginia, this argument fails." *Id.*

The Court reached a similar conclusion in denying an application to issue a search warrant in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*"). There, the location of the target computer was unknown but the Government relied on Rule 41(b)(1) by reasoning that the "information obtained from the Target Computer will first be examined in this judicial district." *Id.* at 756. In rejecting the application, the court explained that the search and seizure of data occurs "not in the airy nothing of cyberspace, but in physical space with a local habitation and a name." *Id.* The same is true here. The NIT search did not occur in Eastern Virginia or in cyberspace. It was a physical search of the defendant's computer located in Massachusetts.

**2. The Warrant is Not Authorized Under Any of the Other Subsections of Rule 41(b).**

The other subsections of Rule 41(b) are inapplicable to this case.

Rule 41(b)(2)—which allows an extraterritorial search or seizure of moveable property if it is located within the district when the warrant is issued but might move or be moved before the warrant is executed—fails to provide authorization because the defendant’s computer was never physically within the Eastern District of Virginia. See *Michaud*, 2016 WL 337263 at \*6 (finding “unconvincing” the argument that Rule 41(b)(2) applies “given the interconnected nature of communications between Website A and those who accessed it.”). Importantly, the court in *In re Warrant* noted:

That (b)(2) does not authorize a warrant in the converse situation—that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment’s reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.

958 F. Supp. 2d at 757.

Rule 41(b)(3) cannot serve as a basis because this case does not involve terrorism.

Rule 41(b)(4) allows for tracking devices to be installed within the issuing district on an object that may travel to outside the district. The NIT here was installed on the defendant’s computer in Massachusetts, which was never physically located within the Eastern District of Virginia. See *Michaud*, 2016 WL 337263 at \*6. Even if the installation were

deemed to have occurred on the server in Virginia, section (b)(4) is inapplicable because the defendant "never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district." *See id.*

Rule 41(b)(5) does not apply because the defendant's computer was not located within any of the specified areas covered by this subsection.

**3. The Warrant Also Violated 28 U.S.C. § 636(a).**

The search warrant issued by the magistrate judge in the Eastern District of Virginia also was in violation of the Federal Magistrates Act. *See Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring) (emphasizing that a violation of Rule 41(b)'s territorial limitations also implicates a statutory limitation). Section 636(a) provides three geographic areas in which a magistrate judge's powers are effective, none of which applies here. *See id.*<sup>4</sup> Thus, the NIT Warrant not only violated Rule 41, but also Section 636(a) of the Federal Magistrates Act.

---

<sup>4</sup>"Each United States Magistrate judge ... shall have [1] within the district in which sessions are held by the [district] court that appointed the magistrate judge, [2] at other places where that [district] court may function, and [3] elsewhere as authorized by law ... all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure. . . ." *Id.*

**B. The Violation of Rule 41 Requires Suppression.**

Suppression is required because the Rule 41 violation also implicates Section 636(a). See 28 U.S.C. 636(a). The issuing magistrate judge lacked statutory authority to issue the NIT warrant in the first place. See *Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring). Importantly, "Section 636(a)'s territorial restrictions are *jurisdictional* limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation—quite unlike the violation of a more prosaic rule or statute—is *per se* harmful." *Id.* at 1122 (emphasis in original).

Our whole legal system is predicated on the notion that good borders make for good government, that dividing government into separate pieces bounded both in their powers and geographic reach is of irreplaceable value when it comes to securing the liberty of the people.

*Id.* at 1125, citing *Bond v. United States*, 564 U.S. 211 (2011); The Federalist Nos. 28, 32 (Alexander Hamilton), Nos. 46, 51 (James Madison).

The magistrate judge was never authorized to issue the NIT warrant and therefore its use constitutes Government hacking of the defendant's computer. Indeed, "a warrant issued in defiance of positive law's jurisdictional limitations on a magistrate judge's powers . . . for Fourth Amendment purposes. . . . is no warrant at all." See *Krueger*, 809 F.3d at 1126 (Gorsuch, J., concurring). This violation of a jurisdictional statute mandates

suppression to preserve judicial integrity and proper separation of powers under the United States Constitution. See *id.* at 1123 (noting that § 636 is entitled "Jurisdiction, powers, and temporary assignment").

Moreover, violations of Rule 41 require suppression when a defendant is prejudiced by the lack of compliance. See *United States v. Bonner*, 808 F.2d 864, 869 (1st Cir. 1986). "Prejudice means being 'subjected to a search that might not have occurred or would not have been so abrasive' had the rules been followed." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015), quoting *Bonner*, 808 F.2d at 869.

In the instant case, the defendant was prejudiced because the search authorized by the Residential Warrant would never have occurred but for information derived from the improperly issued NIT Warrant. Investigators discovered the defendant's alleged IP address through the use of the NIT. See Exh. 1 at ¶ 27. They then used this information to obtain the subscriber information for the IP address from Verizon, which ultimately led them to obtain the Residential Warrant. *Id.* at ¶ 29. The sole reason that investigators were able to identify the defendant as a suspect is because they had already used the NIT Warrant to search his computer and obtain his IP address. Thus, if not for the NIT Warrant, there would have been no probable cause to support the Residential Warrant. Exh. 2 at ¶ 58

("deployment of a NIT to attempt to identify actual IP addresses used by TARGET SUBJECTS . . . is *the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the identity of the TARGET SUBJECTS.*") (emphasis added). The search of the defendant's property conducted on August 12, 2015 would therefore never have occurred.

The unrestrained expansion of judicial authority to issue search warrants without geographic limitation is not a mere technicality. This violation of Rule 41(b) is not the type of "ministerial" violation for which courts have declined to require suppression. *See e.g., United States v. Dauphinee*, 538 F.2d 1, 3 (1st Cir. 1976) (steps required by Rule 41(d) are basically ministerial). The Court exceeded its authority by issuing a warrant for property located outside of its jurisdiction.

The Court of Appeals for the District of Columbia considered a similar issue in *United States v. Glover*, 736 F.3d 509, 510-516 (D.C. Cir. 2014) where it suppressed the fruits of a Title III wiretap because the court had authorized the installation of a listening device outside of the District. The Court held that Rule 41(b), which partially implements Title III, is "crystal clear" and that "a jurisdictional flaw in the warrant" cannot be excused as a "technical defect." *Id.* at 515.

The same logic applies with even greater force here. The agents in *Glover* could have simply obtained the warrant from a magistrate judge in Maryland or Virginia whereas in this case there is no magistrate judge with authority to issue the nationwide warrant.

Moreover, the court in *Glover* found a "blatant disregard of a district judge's jurisdictional limitation" where the warrant expressly authorized agents to enter the vehicle regardless of whether it was located in D.C., Maryland, or Virginia. 736 F.3d at 510, 515. In the instant case, the Government failed to comply with the Fourth Amendment's particularity requirements. *U.S. Const. Amend. IV* ("no warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched. . ."). The "manifest purpose of the particularity requirement of the Fourth Amendment is to prevent wide-ranging general searches by the police." *Bonner*, 808 F.2d at 866. Had the government particularly described the place to be searched, i.e., a computer in Massachusetts, no warrant could have issued. Instead, the search warrant erroneously described the place to be searched as the server, located in Virginia. See Exh. 3 Attachment A. Similarly, it described the information to be seized as data from the activating computers while overlooking the fact that such information could only be obtained by first

searching and seizing the data from those computers. See Exh. 3 Attachment B.

"The test for determining the adequacy of the description of the location to be searched is whether . . . 'there is any reasonable probability that another premise might be mistakenly searched.'" *Bonner*, 808 F.2d at 866. Because the magistrate in Virginia could not authorize a search of a computer in Massachusetts, its occurrence demonstrates that the description was insufficient to prevent a reasonable probability of mistake. The fact that countless other computers were also searched only bolsters this conclusion. When it comes to a constitutional concern such as the particularity requirement, the Government cannot be rewarded for vagueness. To do so would invite further violations and undermine the core requirement set forth in the Fourth Amendment. See *In re Warrant*, 958 F. Supp. 2d at 758 ("This particularity requirement arose out of the Founders' experience with abusive general warrants").

Finally, the officers acted in intentional and deliberate disregard of Rule 41. Even where no prejudice occurs, suppression is appropriate where the government was not acting in good faith. See *United States v. Leon*, 468 U.S. 897, 922 (1984); *Krawiec*, 627 F.2d at 582; *Dauphinee*, 538 F.2d at 3. Particularly where the Government moved Website A's server from North Carolina to Virginia, there can be no credible argument

that officers reasonably believed that none of the 214,898 members of Website A were located outside of Virginia. See Exh. 3 Attachment A ("The activating computers are those of *any user or administrator* who logs into the TARGET WEBSITE.") (emphasis added); Exh. 2 at ¶ 71 ("It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside.").

It is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located outside the authorizing district. In *In re Warrant*, the court stated that where the location of the Target Computer is unknown, "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." 958 F. Supp. 2d at 757. It is unlikely that the Government was unaware of this opinion when it filed its application.

In any event, the Government was clearly aware that the NIT Warrant was not authorized when it made its application in February, 2015. A memorandum addressed to the Committee on Rule of Practice and Procedure dated May 5, 2014, introduces a proposed amendment to Rule 41(b) that would authorize the use of the NIT Warrant. See Reena Raggi, *Report of the Advisory Committee on Criminal Rules*, May 5, 2014, at 319.<sup>5</sup> Specifically, proposed Rule 41(b)(6) "would authorize a court to issue a

---

<sup>5</sup> Available at: <http://www.fpd-ohn.org/sites/default/files/Preliminary%20Draft%20of%20Proposed%20Fed%20Rule%20Amendments%2015Aug2014.pdf>.

warrant to use remote access to search electronic storage media and seize electronically stored information inside or outside of the district: (1) when a suspect has used technology to conceal the location of the media to be searched." Rebecca A.

Womeldorft, *Transmittal of Proposed Amendments to the Federal Rules*, Oct. 9, 2015, at 8.<sup>6</sup> Where the memorandum introducing the proposal states that the change "had its origins in a letter from Acting Assistant Attorney General Mythili Raman," it is not feasible that the Government was unaware that such searches were not authorized under Rule 41(b). See *Report of the Advisory Committee on Criminal Rules*, at 324. Perhaps most telling, the memorandum states that the reason for the proposal is that the territorial venue provisions create "special difficulties" for the Government when investigating crimes involving electronic information. *Id.* at 325 (explaining that "a warrant for a remote access search when a computer's location is not known would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device."). The fact that the proposal requires an entirely new subsection to Rule 41(b), rather than a clarification to an existing subsection, demonstrates that there is no reasonable interpretation of any provision in Rule 41(b) that would permit such a search.

---

<sup>6</sup> Available at: <http://www.uscourts.gov/file/18641/download>.

Rule 41(b) provides explicit geographic limits on the magistrate judge's authority to issue search warrants and, under the circumstances presented here, precluded her from issuing a warrant authorizing the search of property outside the district. The rule is clear. It is not for this Court to rewrite it to keep up with new technological developments. It is for the United States Congress<sup>7</sup> to address any shortcomings in the Rule. Until that occurs, searches like the one in this case violate Rule 41(b) and must result in suppression.

**CONCLUSION**

WHEREFORE, the defendant moves that the Court suppress all evidence obtained as a result of the search and seizure authorized by Search Warrant #15-MJ-2187.

ALEX LEVIN  
By his attorneys,  
CARNEY & ASSOCIATES

*J. W. Carney, Jr.*

J. W. Carney, Jr.  
B.B.O. # 074760

Nathaniel Dolcort-Silver  
B.B.O. # 693968  
20 Park Plaza, Suite 1405  
Boston, MA 02116  
617-933-0350  
jcarney@CARNEYdefense.com

---

<sup>7</sup>See generally *Krueger*, 809 F.3d at 1119-21 (Gorsuch, J., concurring)(need for Congressional approval).

February 18, 2016

Certificate of Service

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on or before the above date.

*J. W. Carney, Jr.*

J. W. Carney, Jr.

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

_____	)	
UNITED STATES OF AMERICA	)	
	)	
V.	)	Crim. No. 15-cr-10271-WGY
	)	
ALEX LEVIN	)	
_____	)	

**AFFIDAVIT SUPPORTING**  
**DEFENDANT'S MOTION TO SUPPRESS EVIDENCE**

I, J. W. Carney, Jr., state that the facts contained in the attached motion are true to the best of my information and belief.

Signed under the penalties of perjury.

*J. W. Carney, Jr.*  
J. W. Carney, Jr.

February 18, 2016