

UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

UNITED STATES OF AMERICA)
)
) CR-09-38-B-W
)
)
GARY FARLOW)

**ORDER AFFIRMING THE RECOMMENDED DECISION
OF THE MAGISTRATE JUDGE**

On September 29, 2009, the United States Magistrate Judge filed with the Court her Recommended Decision in which she recommended that the Court deny Mr. Farlow’s Motion to Suppress Evidence Obtained as a Result of Illegal Seizure and Search (Docket # 29) (*Def.’s Mot.*). *Recommended Decision* (Docket # 43) (*Rec. Dec.*). The Magistrate Judge also denied Mr. Farlow’s request for an evidentiary hearing on his motion. *Rec. Dec.* at 8-9. Mr. Farlow filed his objection to the Recommended Decision on October 13, 2009. *Def.’s Obj. to Report and Recommendation* (Docket # 44) (*Def.’s Obj.*). The Government responded to the Defendant’s objections on October 30, 2009. *Resp. of the United States of America to Def.’s Objections to Report and Recommendation* (Docket # 47) (*Gov’t’s Resp.*) The Court has reviewed and considered the Magistrate Judge’s Recommended Decision, together with the entire record, and has made a *de novo* determination of all matters adjudicated by the Magistrate Judge’s Recommended Decision. For the following reasons and for the reasons set forth in the Magistrate Judge’s Recommended Decision, the Court adopts the Magistrate Judge’s Recommended Decision and denies Mr. Farlow’s motion to suppress.

I. STATEMENT OF FACTS¹

On March 1, 2007, March 8, 2007, and April 14, 2007, Nassau County Detective Peter Badalucco, posing as a 14 year old teenager, “Chris”, received sexually suggestive emails from a person using the AOL screen name “FarlowMeCasa”, that included explicit sexual advances and a request for an in-person meeting. Sending written sexual solicitations to an undercover police officer posing as a 14-year-old boy violates two state of New York criminal statutes: dissemination of indecent materials to a minor in the first degree, N.Y. Penal Stat. § 235.22, and endangering the welfare of a child. N.Y. Penal Stat. § 260.00. In one or more of those emails, “FarlowMeCasa” sent Det. Badalucco a non-pornographic digital photograph of a bodybuilder, claiming it was his photograph. After Det. Badalucco subpoenaed the AOL subscriber information for “FarlowMeCasa” and confirmed that the profile was registered to Gary Farlow of Litchfield, Maine, he contacted Detective Laurie Northrup of the Maine State Computer Crimes Unit (MCCU) on April 13, 2007 to request her assistance in obtaining a search warrant “to seize computers and electronic data storage devices for forensic examination for evidence of these violations of New York criminal laws.” *Resp. of United States of America to Def.’s Suppression Mot.* Attach. 1, *Search Warrant, Aff. of Det. Laurie Northrup of the Maine State Police Computer Crimes Unit* at 5 (Docket # 35).

Detective Northrup made out a search warrant and swore out an affidavit in support of the warrant. *Id.* Detective Northrup’s affidavit highlighted in bold the crimes for which the search warrant was being sought:

All of which constitute evidence of the crimes of disseminating indecent material to minor in the first degree in violation of New York State Statute

¹ The Court has recited only those facts critical to its decision. The details of the case are fully set forth in the Magistrate Judge’s Recommended Decision. *Rec. Dec.* at 1-5.

138-A § 235.22 and endangering the welfare of a child in violation of New York State Statute 138-A § 260.00.

Id. at 4. On April 23, 2007, she presented the request for a search warrant to a state of Maine District Judge, who approved its issuance, authorizing a search of Mr. Farlow's Litchfield residence, his motor vehicles, any persons at the premises, and his computers as follows:

1. Computers and computer equipment (such as monitors, keyboards, compact disk drives, zip disk drives, USB drives, digital cameras, MP3 players, etc.), electronic data storage devices (such as hard drives, floppy disks, zip disks, compact disks, digital video disks, memory sticks, flash memory cards, etc.), software, and written materials relating to the operation of the computer (such as names of online accounts, screen names, passwords, manuals, computer reference books, guides and notes).
2. Computer records or data, whether in printed or electronic form, that are evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a child, including but not limited to records of Internet use (such as Internet browser history, search engine history, temporary Internet files, etc.), electronic communications (such as email and email attachments, records or data pertaining to online chat room communications, file transfer logs, text messages, writing created on word processing software or notepads, etc.), stored data files and folders, graphic visual images (such as photographs, movie clips and scanned images), software or programs for file sharing or peer-to-peer networks, personal calendars or diaries, and any records or data that demonstrate the identity of the person(s) who exercised dominion or control over the computer or its contents.

Id. at 2. Armed with this warrant, Det. Northrup searched Mr. Farlow's Litchfield residence during the afternoon of April 23, 2007. As Det. Northrup began to execute the search, Mr. Farlow was on-line with Det. Balalucco, and the New York Detective was communicating directly with Det. Northrup by cell phone. Mr. Farlow admitted that he had been chatting with "Chris" in New York, and that he had been doing so when the police arrived. Detective Northrup seized Mr. Farlow's computer and removed it to the MCCU.

On April 24, 2007, Sergeant Glenn Lang of the MCCU performed an initial search of Mr. Farlow's computer. When the sergeant conducted the search for the bodybuilder image that "FarlowMeCasa" had sent to "Chris", digital images of child pornography appeared on the

screen. Based on these images, Sgt. Lang sought and obtained a second search warrant that permitted a search for images of child pornography.

The nub of Mr. Farlow's motion to suppress is that Sgt. Lang could and should have limited his search to the bodybuilder image itself. If Sgt. Lang had done so, under his theory, the search would have revealed the bodybuilder's non-pornographic image, but not the images of child pornography. Asserting that the warrant did not sufficiently limit the computer search, Mr. Farlow says it violated the particularity requirement of the Fourth Amendment.

II. DISCUSSION

A. The Demand for an Evidentiary Hearing

The Magistrate Judge decided Mr. Farlow's motion to suppress without an evidentiary hearing. *Rec. Dec.* She stated:

There is no need for a hearing to support a finding that Sgt. Lang could have focused his investigation on the AOL chat room communications, which may have or would have turned up evidence of the body builder image directly co-located with the pertinent criminal communications data.

Id. at 8-9. Mr. Farlow earnestly contends that the Magistrate Judge erred in refusing to allow an evidentiary hearing, relying instead on Sergeant Lang's uncross-examined affidavit:

Were the defense able to question Sgt. Lang regarding the nature of hash values and the search protocols available through the use of Encase software, it is believed that Sgt. Lang would have to admit that he had access to the digital image received by the undercover agents in New York, that he could have run a scan for a digital match of that version of the digital image, and that he in fact did find a match for that particular image. This is due to the nature of the Encase program and its ability to seek out those images that possess particular hash values.

Def.'s Obj. at 2.

The standard for determining whether to grant "an evidentiary hearing in a criminal case [is] substantive: did the defendant make a sufficient threshold showing that material facts were

in doubt or dispute?” *United States v. Allen*, 573 F.3d 42, 50 (1st Cir. 2009) (quoting *United States v. Vilches-Navarrete*, 523 F.3d 1, 15 (1st Cir. 2008)). To obtain an evidentiary hearing, the “burden is on the defendant to allege facts, sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.” *United States v. Calderon*, 77 F.3d 6, 9 (1st Cir. 1996) (internal quotation marks and citation omitted).

Rule 47(b) allows a party making a motion to support it “by affidavit.” Fed. R. Crim. P. 47(b). Here, however, Mr. Farlow elected not to present any affirmative evidence to contradict the declaration of Sgt. Lang concerning the practical parameters of his search of the Farlow computer. For example, there is no expert defense witness affidavit describing an alternative and less invasive search protocol and contradicting Sgt. Lang’s declaration. Instead, Mr. Farlow’s defense counsel asserts in the objection what Sgt. Lang “would have to admit” during cross-examination at the suppression hearing. *Def.’s Obj.* at 2. But, defense counsel’s say-so alone is not enough to mandate an evidentiary hearing, particularly in the context of expert evidence.

The First Circuit has noted that a district court is not required to accept “unsupported factual assertions in [a defendant’s] memorandum of law,” where the memorandum does “not contain any record citations that would have confirmed these allegations.” *Allen*, 573 F.3d at 52. This situation is similar to *Calderon* where the defendant “vaguely claim[ed]” that consent to search was “coerced or was otherwise ineffective,” but offer[ed] no affidavit or statement . . . to that effect, describe[d] no circumstances supporting his assertion, and ma[de] no offer of proof relative to any other facts that might support his assertion.” *Calderon*, 77 F.3d at 9. In effect, defense counsel seeks to generate an evidentiary hearing by proffering her own expertise in the area of computer searches, and making an assured pronouncement that the Government’s expert would capitulate on the stand and concede that her understanding of computer searches is correct

and his earlier declaration in error. The Court is not required to accept unverified assertions in counsel's memorandum; the Court is allowed to accept "only the verified evidence before it."² *Allen*, 573 F.3d at 52. Mr. Farlow has not alleged "facts, sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented," *id.* at 50, and has not by counsel's assertions alone generated the need for an evidentiary hearing.

B. The Fourth Amendment's Particularity Requirement

The gist of Mr. Farlow's argument is that the Encase software program that Sgt. Lang used to perform the computer search allows an investigator to track down a digital image based on its unique hash mark. As Mr. Farlow sent the bodybuilder photograph to Det. Badalucco, posing as "Chris", the police had access to the hash mark of the digital image, also known as the digital fingerprint. Mr. Farlow says that all Sgt. Lang had to do was to enter the hash mark into the Encase program and the program would have revealed the presence of the same bodybuilder digital photograph on Mr. Farlow's computer. Once law enforcement confirmed that the bodybuilder photograph with its digital fingerprint was on both Mr. Farlow's and the New York Detective's computers, there would have been no justification for continuing to search Mr. Farlow's computer, since the purpose of the search was limited to the New York State crimes delineated in Det. Northrup's affidavit. In other words, authorization to search a computer for a non-pornographic image of a bodybuilder does not include authorization to search for images of child pornography.

² Defense counsel states that "[i]f the court decides to dispose of this motion on the basis that Mr. Farlow has not presented evidence that Sgt. Lang could have performed a more limited search, he represents that he could make such a factual basis at a hearing." *Def.'s Obj.* at 3 n.1. The Court does not accept this unverified proffer. It is not a statement of probative evidence; it is a statement of hope. There is a difference between evidence counsel knows she will present by witness or exhibit, and concessions counsel hopes to elicit from a government expert witness on cross-examination.

This factual argument translates into a legal contention under the Fourth Amendment’s particularity requirement. The Fourth Amendment’s Warrants Clause provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV; *United States v. Rogers*, 521 F.3d 5, 9 (1st Cir. 2008) (quoting U.S. Const. amend. IV). “Any search intruding upon [an individual’s] privacy interest must be justified by probable cause and must satisfy the particularity requirement, which limits the scope and intensity of the search.” *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986). The Fourth Amendment’s particularity requirement focuses on two concerns: “one is whether the warrant supplies enough information to guide and control the agent’s judgment in selecting what to take, and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized.” *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (citations omitted).

In requiring a particular description of articles to be seized, the Fourth Amendment “makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *United States v. Fuccillo*, 808 F.2d 173, 175 (1st Cir. 1987) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Unfettered discretion by the executing officer is one of the principal evils against which the Fourth Amendment provides protection, and thus warrants which lack particularity are prohibited.

United States v. Morris, 977 F.2d 677, 681 (1st Cir. 1992).

Mr. Farlow first contends that the warrant itself was overbroad. The Court disagrees. The warrant itself authorizes a search of “[c]omputer records or data, whether in printed or electronic form, that are evidence of the crimes of dissemination of indecent materials to minors or endangering the welfare of a child. . . .” *Search Warrant* at 2 (emphasis added). The warrant did not allow a general search of the Farlow computer; it limited the search to evidence of the

crimes under investigation. As the Magistrate Judge explained, “[a]uthorization of a search of the computer was particular to the computer crime at issue.” *Rec. Dec.* at 7.

This limitation distinguishes this case from *United States v. Otero*, 563 F.3d 1127 (10th Cir. 2009), where the appeals court recently reinforced the principle that “warrants for computer searches must *affirmatively limit* the search to evidence of specific federal crimes.” *Id.* at 1132 (citation omitted). Unlike *Otero*, the “most practical reading” of this warrant would not “authorize[] a wide-ranging search of [the defendant’s] computer.” *Id.* at 1133. Rather, here, the warrant stipulated the potential crimes for which the warrant was authorized: the dissemination indecent material to minors and endangering the welfare of a child. Thus, since the warrant stated the specific criminal activity likely to be found on Mr. Farlow’s computer, it “cannot be classified as a generic classification that would go against the particularity requirement of the Fourth Amendment.” *Upham*, 168 F.3d at 536 n.1 (stating that a search warrant with the “qualifying language” of the offense at issue “leave[s] ‘little latitude’ to the executing officers and [is] sufficiently particular to satisfy the Fourth Amendment”); *see also United States v. Crespo-Rios*, 623 F. Supp. 2d 198 (D.P.R. 2009); *United States v. Cameron*, CR-09-24-B-W, 2009 U.S. Dist. LEXIS 79684, at *12 (D. Me. Sept. 1, 2009). Moreover, when faced with a similar allegation of an overbroad warrant, the First Circuit upheld the search of a computer and co-located disks. *Upham*, 168 F.3d at 535 (stating that “[a] search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs”).

Mr. Farlow has another arrow in his quiver. He contends that the search warrant was fatally defective, because it did not restrict the type of search that the officers could make of the Farlow computer. The Magistrate Judge considered this issue and concluded that “[i]mposing a

search protocol to restrict a computer search is something that a judge may do in an appropriate case. However, I cannot say that the state judge's failure to impose a search protocol prohibiting a visual scan of image files resulted in an overbroad warrant. . . ." *Rec. Dec.* at 10.

The Supreme Court has long recognized that document searches pose unique problems:

[T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.... [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). With the advent of the computer age, courts have struggled to balance privacy interests against law enforcement interests. *United States v. Cioffi*, No. 08-CR-415 (FB), 2009 U.S. Dist. LEXIS 99409, at *14-15 (E.D.N.Y. Oct. 26, 2009) (stating that "[c]ourts and commentators have wrestled with how best to balance privacy interests and legitimate law-enforcement concerns in the context of computer searches"). In *Cioffi*, the district court discussed two approaches. "One approach would require law-enforcement officials to specify a search protocol *ex ante* and to use, whenever possible, 'key word searches . . . to distinguish files that fall within the scope of a warrant from files that fall outside the scope of the warrant.'" *Id.* at *15 (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 108 (1994)). Another "would require the creation of 'firewalls' to prevent investigators and prosecutors from obtaining the results of a computer search until documents within the scope of the warrant had been segregated by a third party." *Id.*

A similar issue recently came to a head in the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (*CDT*), an en banc opinion.

CDT involved a federal investigation into steroid use by professional baseball players. The Ninth Circuit described the case as being about “the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information.” *Id.* at 993. *CDT* administered a steroid testing program for the Major League Baseball Players Association, and after the Government learned that ten players had tested positive for steroid use, it sought and obtained a subpoena limited to the records of those ten players. *Id.* After the players and *CDT* moved to quash the subpoena, the government “obtained a warrant in the Central District of California authorizing the search of *CDT*’s facilities in Long Beach. Unlike the subpoena, the warrant was limited to the records of the ten players as to whom the government had probable cause. When the warrant was executed, however, the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people).” *Id.*

The Ninth Circuit concluded that *CDT* was “an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause.” *Id.* at 1000. To prevent the Government overreaching in the future, the Ninth Circuit imposed stringent requirements including that the government should “forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data,” *id.* at 998, and that the warrant application “should normally include, or the judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown.” *Id.* at 1000. The Ninth Circuit suggested that an independent expert or special master segregate the material, and allow the investigating officers to search only the information responsive to the warrant. *Id.*

Admittedly, if *CDT* applied here, and the Government had forsworn or been ordered to forswear the plain view doctrine in searching, and a third party had segregated all photographs not directly related to the search for evidence of the state of New York crimes, either Sgt. Lang would not have discovered the child pornography or the third party would have been compelled not to have disclosed its existence. But, no other circuit has gone as far as the Ninth to require such significant preconditions on the issuance of search warrants for computers.³ In the Court's view, the far preferable approach is to examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a motion to suppress. If the police conduct is as egregious as the Ninth Circuit found in *CDT*, the Court can consider appropriate remedies. This fact-intensive, considered

³ From this Court's perspective, *CDT* creates more problems than it solves. No doubt, the police misconduct in *CDT* was egregious; in *CDT*, the Ninth Circuit concluded that the police deliberately overreached and seized evidence for which they had no probable cause. But, the traditional sanction for police misconduct of this sort remains exclusion of evidence. See *Weeks v. United States*, 232 U.S. 383, 398 (1914); *United States v. Calandra*, 414 U.S. 338, 347-48 (1974). Although "suppression is not an automatic consequence of a Fourth Amendment violation," *Herring v. United States*, 129 S. Ct. 695, 698 (2009), the Supreme Court has also said that "[t]he extent to which the exclusionary rule is justified by . . . deterrence principles varies with the culpability of the law enforcement conduct." *Id.* at 701. In *Hudson v. Michigan*, 547 U.S. 586, 597-98 (2006), the Supreme Court, though constraining the scope of the exclusionary rule, noted that 42 U.S.C. § 1983 provides a civil remedy for police violations of constitutional rights. The *CDT* protocols impose extraordinary precautions against police misconduct for all applications for a warrant to search a computer, assuming misconduct will be the rule, not the exception. There is no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures, and at the very least the more traditional remedies should be tried first.

Moreover, *CDT* requires the issuing judicial officer to "insert[] a protocol for preventing agents . . . from examining or retaining any data other than that for which probable cause is shown." *CDT*, 579 F.3d at 1000. Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case, and the notion that a busy trial judge is going to be able to invent one out of whole cloth or to understand whether the proposed protocol meets ill-defined technical search standards seems unrealistic.

Finally, to require that the Government forswear the plain view doctrine is, in the Court's view, an extreme remedy better reserved for the unusual, not common case. In *CDT*, the ill-gotten evidence was of baseball players' use of steroids, certainly a matter of notoriety, but relatively benign in the scope of federal criminality. Here, the evidence in plain view on Mr. Farlow's computer is child pornography, the possession of which is a serious federal felony. In a future case, the evidence in plain view could be profoundly serious, ranging from photographs of a kidnapped child to plans to commit acts of terrorism. The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair. To require the government before every computer search to forswear the plain view doctrine, which itself has its own constraints, seems unwise.

analysis is what *Upham* contemplates. *Upham*, 168 F.3d at 536 (stating that “[t]his problem arises in a variety of different contexts and in many permutations; matters of degree are involved and there is probably no single rule that resolves all such situations”).

In the First Circuit, *Upham* remains the law. *Id.* at 535 (stating that “a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for weapons or drugs”). Whether *Upham* authorizes a deliberate law enforcement search of Mr. Farlow’s computer for child pornography under the guise of a search for a single non-pornographic digital photograph of a bodybuilder is highly questionable.⁴ *Id.* (stating that “[t]he requirement of particularity arises out of a hostility to the Crown’s practice of issuing ‘general warrants’ taken to authorize the wholesale rummaging through a person’s property in search of contraband or evidence”).

But, at least in the narrow context of this motion to suppress, Mr. Farlow’s argument fails on the facts. *Id.* at 636 (stating that “[t]his problem arises in a variety of different contexts and in many permutations; matters of degree are involved and there is probably no single rule that resolves all situations”). Here, Sgt. Lang has declared under the penalty of perjury “[t]he only reasonable way for an examiner to locate most of the copies of a particular image is to do it visually.” *Decl. of Glenn Lang* at 2. Sgt. Lang rejected the defense assertion that tracking the hash mark would have led to the bodybuilder photograph, since “[e]very time one pixel of a picture is changed the hash value is completely different. If the user were to open the picture and save it to another location with a picture viewer, the hash can be changed via compression.

⁴ It is not inconceivable that Sgt. Lang, realizing that Mr. Farlow was soliciting sex from a presumed minor over the internet, was suspicious that he might also possess child pornography, and used a computer search protocol that gave him the ability to view other images, finding by indirection what he would not have been able to look for directly. But, the record is silent as to the efficacy of other protocols and whether the visual inspection Sgt. Lang used in this case is standard operating procedure or something out of the ordinary. Absent countervailing evidence, the Court will not assume Sgt. Lang was gaming the restrictions in the warrant.

When a file is deleted, its hash value changes.” *Id.* Based on this evidence, Sgt. Lang’s method of searching the Farlow computer was “about the narrowest definable search and seizure reasonably likely to obtain the images.” *Upham*, 168 F.3d at 535. This is especially true here, where, as the Magistrate Judge pointed out, *Upham* emphasized that “[t]he warrant process is primarily concerned with identifying *what* may be searched or seized - - not how - - and *whether* there is sufficient cause for the invasion of privacy thus entailed.” *Id.* at 537 (emphasis in original).

Ultimately, the Court arrives at the same conclusion as the Magistrate Judge. Once the contents of Sgt. Lang’s declaration are conceded, his search protocol does not violate Fourth Amendment particularity requirements, and when he visually tripped over evidence of the commission of other crimes in plain view, he was not required to ignore it. *United States v. Parker*, 549 F.3d 5, 10 (1st Cir. 2009) (endorsing the plain view doctrine).

III. CONCLUSION

1. It is therefore ORDERED that the Recommended Decision of the Magistrate Judge (Docket # 43) is hereby AFFIRMED.
2. It is further ORDERED that the Defendant’s Motion to Suppress Evidence (Docket # 29) is DENIED.

SO ORDERED.

/s/ John A. Woodcock, Jr.
JOHN A. WOODCOCK, JR.
CHIEF UNITED STATES DISTRICT JUDGE

Dated this 3rd day of December, 2009

Defendant (1)

GARY A FARLOW

represented by **VIRGINIA G. VILLA**
FEDERAL DEFENDER'S OFFICE
KEY PLAZA, 2ND FLOOR
SUITE 206
23 WATER STREET
BANGOR, ME 04401
(207) 992-4111 Ext. 102
Email: Virginia_Villa@fd.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Public Defender or
Community Defender Appointment

Plaintiff

USA

represented by **JAMES M. MOORE**
OFFICE OF THE U.S. ATTORNEY
DISTRICT OF MAINE
202 HARLOW STREET, ROOM 111
BANGOR, ME 04401
945-0344
Email: jim.moore@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED