BRIAN J. STRETCH (CABN 163973)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JOSEPH M. ALIOTO, JR. (CABN 215544)
WILLIAM FRENTZEN (LABN 24421)
SCOTT D. JOINER (CABN 223313)
BRIGID S. MARTIN (CABN 231705)
Assistant United States Attorneys

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (415) 436-7200
Fax: (415) 436-6753
Joseph.Alioto@usdoj.gov
William.Frentzen@usdoj.gov
Scott.Joiner@usdoj.gov
Brigid.Martin@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. PURVIS LAMAR ELLIS, et al., Defendants.	CR 13-00818 PJH DECLARATION [redacted]

I, [redacted], declare as follows:

(1) I am a Special Agent with the Federal Bureau of Investigation. I have been assigned to the FBI's San Francisco Division Technical Program since November 2003 and have been employed by the FBI in its San Francisco Division since 1997. My work for the FBI's Technical Program involves using developing technology to conduct legally-authorized collections of evidence in support of FBI investigations. The FBI's Technical Program is also authorized to lend technical assistance to state and local agencies conducting criminal investigations.

(2) In many instances, the technical investigative techniques used by the FBI's Technical Program are used in support of covert investigations and utilize law enforcement sensitive techniques that are protected under the qualified "law enforcement sensitive" privilege under federal law. In addition, the identity of technically-trained agents are protected under the same privilege and they are considered covert assets by the FBI.

(3) Because of the nature of my official duties, I am familiar with the matters at issue in this case. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(4) Law enforcement agents can use cell site simulators to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from devices in the simulator operator's vicinity. This technology is one tool among many traditional law enforcement techniques available to law enforcement. In support of the FBI San Francisco Division's Technical Program, I have been trained in the operation of cell site simulator technology.

(5) In general, cell site simulators function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most "attractive" cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.

(6) A cell site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular

device (as occurred in this case), a cell site simulator initially receives the unique identifying numbers from multiple devices in the vicinity of the simulator. For the provider in this case, this number is known as a Mobile Identification Number ("MIN").[1] Once the cell site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone.

(7) By transmitting as a cell tower, cell site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell site simulators used by Federal, state, and local law enforcement agencies must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself. The cell site simulator does not remotely capture e-mails, texts, contact lists, images, or other data from the phone, nor does it, as configured, provide subscriber account information (such as an account holder's name, address, or telephone number).

(8) On January 22, 2013, I received a telephonic request from a FBI Oakland Residence Agency criminal squad located in Oakland, California. To the best of my knowledge, I believe I received this request around 7:00 AM. The request indicated that an Oakland Police Officer had been shot in the vicinity of 1759 Seminary Street, Oakland, California and that the subject had not been apprehended. I was notified that Oakland Police Department was requesting FBI assistance in the use of its cell site simulator.

(9) In response to that request, I contacted the telephone carrier of the subject cellular telephone and completed the required exigent circumstance request form to obtain a pen register/trap trace and subscriber information, including the MIN, for phone number 510-904-7509 to assist in

[1] The MIN is generally different than the phone number of the device, though sometimes it can be the same. My review of subscriber information for the targeted device in this case indicates that the MIN was not the same as the target phone number. For devices other than the targeted device, however, I would not have known at the time whether the MINs encountered by the cell site simulator were the same as the device phone numbers or different.

locating the cellular telephone in conjunction with the cell site simulator. I simultaneously requested FBI approval to deploy the cell site simulator in support of Oakland Police Department.

(10) Upon FBI approval to deploy the cell site simulator, I believe I arrived in the vicinity of 1759 Seminary Street, Oakland, California, at approximately 9:00 a.m., on January 22, 2013, with another FBI Special Agent who is also trained to operate the cell site simulator. At approximately 10:00 a.m., the cell site simulator was powered on and operated for approximately one (1) hour. It was configured to look for the MIN for phone number 510-904-7509. After that, the cell site simulator was shut down.

(11) Upon powering the cell site simulator on, it detected the presence of the subject cellular telephone within the apartment building located at 1759 Seminary Street, Oakland, California. Once the cell site simulator identified the subject cellular device, it only obtained the signaling information relating to that particular phone. As previously noted, such signaling information did not include content such as e-mails, texts, contact lists, images, or other data from the phone, nor did it provide subscriber account information.

(12) At one point, in an effort to reduce the error radius and increase the accuracy of the location of the cellular telephone, a cell site simulator augmentation device was deployed into the interior of the apartment building. This device is used in conjunction with the cell site simulator and has no data storage capability whatsoever. As before, during this operation of the cell site simulator, only limited signaling data and identifying information was collected from the targeted cellular telephone. At all times during the deployment of the cell site simulator and the augmentation device, the equipment and I were located in publicly accessible areas in and around the target apartment building.

(13) In line with general FBI policy and practice, the cell site simulator equipment was not configured to collect any content contained on or transmitted by the target device or any other device in the vicinity, e.g. e-mails, texts, contact lists, images, or other data from the phone. In addition, the cell site simulator, as configured, did not collect subscriber account information (such as an account holder's name, address, or the telephone number associated with the device) or collect voice or other audio communications from any device in the area, including the targeted device.

//

(14) Pursuant to FBI policy, all data for this incident was purged at approximately 11:00 a.m. on January 22, 2013, once I had been learned that the subject was arrested and in custody. Purging is done by the FBI as an additional, internal procedural safeguard:

1. to ensure that the privacy rights of innocent third parties are maintained;
2. to ensure that the FBI does not store or maintain data beyond the scope of its legal authorization;
3. to ensure that the FBI does not retain information about individuals who are not the subject of criminal or national security investigation; and
4. to promptly preserve the operational use of the equipment (the equipment cannot be used on another mission until the data from prior missions has been purged. Otherwise, the data from the prior missions would be co-mingled with the non-purged data from prior missions, interfering with the effective use of the data pertaining to each, individual operation).

Consistent with these policy goals, no data was retained in the cell site simulator regarding the subject matter of the operation described above.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing it true and correct to the best of my knowledge.

Executed this 22nd day of August, 2016 in Martinez, California.

[redacted]
Special Agent
Federal Bureau of Investigation