Bradley S. Morrison, being duly sworn, deposes and states:

I am a Supervisory Special Agent (SSA) with the Federal Bureau of Investigation (FBI), currently assigned as the Chief, Tracking Technology Unit, Operational Technology Division (OTD) in Quantico, Virginia. I have been employed as a FBI Special Agent since 1996. As Unit Chief, I am responsible for the development, procurement, deployment, and management of technical assets and capabilities to surreptitiously locate, tag, and track targets of interest in support of all FBI investigative, intelligence collection, and operational programs. I am responsible for establishing and advising on policy guidance for the FBI, including whether a particular tool or technique my program manages meets the criteria for protection as law enforcement sensitive, while ensuring that state-of-the-art technical investigative assets remain available to field technical programs to enable them to assist in a wide range of technical investigative missions. This includes the use and deployment of electronic surveillance devices such as the cell site simulator at issue in this case.

Title 5, United State Code, Section 301 empowers the head of an executive department to set regulations that govern the dissemination of information belonging to that department. With respect to the FBI, as a component of the Department of Justice (DOJ), the Attorney General has promulgated 28 C.F.R. §16.21, in which the Attorney General set forth procedures to follow upon receiving a request for information relating to material contained in the files of the department, or acquired from the department as part of one's official duties. DOJ officials are required to consider several factors in deciding whether to allow privileged information to be released, including whether disclosure of the information sought would "reveal investigatory records compiled for law enforcement purposes, and would... disclose investigative techniques and procedures" whose effectiveness would be impaired by disclosure. 28 C.F.R. §16.26(b)(5).

The FBI OTD has always asserted that the cell site simulators are exempt from discovery pursuant to the "law enforcement sensitive" qualified evidentiary privilege, as information concerning this equipment, if made public, could easily impair use of this investigative method. Likewise, the FBI protects information about its use of this technology in response to requests under the federal Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. Law enforcement techniques and procedures enjoy categorical protection under FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), in order to preserve the utility of those techniques and procedures, and mitigate the risk that they will be circumvented. Under FOIA Exemption 7(E), the FBI protects a range of information about cell site simulators, including operational details such as how, when, where, and under what circumstances the FBI uses cell site simulators, and technical details, such as the particular technology and equipment that the FBI uses. Disclosure of even minor details about the use of cell site simulators may reveal more information than their apparent insignificance suggests because, much like a jigsaw puzzle, each detail may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself. Thus, disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information about the capabilities, limitations, and circumstances of their use, and would allow those adversaries to accumulate information and draw conclusions about the

BSM

use and technical capabilities of this technology. In turn, this would provide them the information necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology. Doing so would thus allow them to evade detection by law enforcement and circumvent the law.

In recognition of this vulnerability, the FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed. The FBI routinely asserts the law enforcement sensitive privilege over cell site simulator equipment because discussion of the capabilities and use of the equipment in court would allow criminal defendants, criminal enterprises, or foreign powers, should they gain access to the items, to determine the FBI's techniques, procedures, limitations, and capabilities in this area. This knowledge could easily lead to the development and employment of countermeasures to FBI tools and investigative techniques by subjects of investigations and completely disarm law enforcement's ability to obtain technology-based surveillance data in criminal investigations. This, in turn, could completely prevent the successful prosecution of a wide variety of criminal cases involving terrorism, kidnappings, murder, and other conspiracies where cellular location is frequently used. See United States v. Rigmaiden, 845 F.Supp. 982 (D.Ariz. 2012); United States v. Garey, 2004 WL 2663023 (M.D.Ga. Nov. 15, 2004); see also generally FBI's Technical Personnel and Technical Equipment and Use Policy Implementation Guide (0631DPG), sections 1.2.1, 1.2.3, and 1.3, and the FBI's Manual of Investigative Operations and Guidelines, §§ 6-2.1, 6-5.3, 10-10.13, 16-4.8.6 and 16-4.8.14.

Further, the FBI has entered into a non-disclosure agreement (NDA) with our state and local law enforcement partners. The NDA is specific to state and local law enforcement use of cell site simulator technology, and was entered into in an effort to protect law enforcement sensitive details about the technology. The NDA acknowledges that "[d]isclosing the existence of and the capabilities provided by [cell site simulator equipment] to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation...to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is, disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such [cell site simulator] equipment continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure...to the public..."

Adding to the sensitive nature of the FBI's cell site simulator equipment, the same techniques and tools used in criminal cases are often used in counterterrorism and counterintelligence investigation. Thus, the compromise of the law enforcement community's investigational tools and

methods in a criminal case or public records disclosure could have a significant detrimental impact on the national security of the United States.

Specifically, any information shared by the federal government with a state concerning cell site simulator technology is considered homeland security information under the Homeland Security Act. The Act defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act. See 6 U.S.C. §§ 482(f)(1)(B)-(D). Cell site simulator technology meets all three criteria. Accordingly, under 6 U.S.C. §482(e), homeland security information "obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information." The FBI does not consent to release of the information, including technical specifications, technique limitations and vulnerabilities, and training and operational materials.

Additionally, cell site simulator technology is a regulated defense article on the United States Munitions List (USML) (see 22 C.F.R. §121.1 – the US Munitions List, Category XI – Military Electronics, subpart (b) – electronic equipment specifically designed for intelligence, security or military use in surveillance, direction-finding of devices which operate on the electromagnetic spectrum). As such, technical details concerning this technology are subject to the non-disclosure provisions of the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. Parts 120-130. The ITAR implements the Arms Export Control Act, 22 U.S.C. §2778, and Executive Order 13637, which control the export and import of defense-related articles and services listed on the United States Munitions List (USML). Because this equipment is explicitly governed by the ITAR, 22 C.F.R. §123.1 requires anyone, prior to making an export, to obtain a license from the Department of State. Notably, technical information does not have to leave the borders of the United States to be deemed an export subject to the regulation. (see 22 C.F.R. §120.17, which defines an export as the disclosure of technical data about a defense article to a foreign national, even while located in the United States).

Accordingly, if a state disseminates any part of the technical information knowing that a media organization intends to release the information to the public through the media or via a website, due to the accessibility of the information to non-US citizens, or the requesting media organization employs or has any non-US citizens present at its offices, this may constitute a violation of the Arms Control Export Act. Any unauthorized disclosure of ITAR-controlled information is a felony punishable by up to 20 years imprisonment and up to $1 million per occurrence. See 22 C.F.R. Part 127.

Specifically, with respect to the cell site simulator used in this case, given the media attention to this case and the inability to control the unauthorized release of information in the internet age, once information about the simulator is publically confirmed, the FBI, as well as the larger law enforcement community, will not be able to employ the equipment again in the future with the same degree of success. Although there is information about cell site simulators and their operation on the Internet, the specific capabilities, settings, limitation and tradecraft used in their deployment were not authoritatively disclosed or confirmed by the FBI. Therefore, should this type of information be

BSM

authoritatively disclosed or endorsed, criminal defendants will gain valuable intelligence on the specific capabilities of the law enforcement community to effect surveillance of and locate individuals.

I declare under penalty of perjury that the foregoing facts are true and correct.

4/11/14

Date

Bradley S. Morrison
Supervisory Special Agent (SSA)
Chief, Tracking Technology Unit
Federal Bureau of Investigation

KELLY A. HADEN COMMONWEALTH OF VIRGINIA NOTARY PUBLIC

Kelly A. Haden
NOTARY PUBLIC
Commonwealth of Virginia
Reg. #353472
My Commission Expires
March 31, 2016

City/County of Stafford
Commonwealth of Virginia
The foregoing instrument was acknowledged before me
this 11 day of April 2014,
by Bradley S. Morrison
Kelly A Haden Notary Public
My commission expires 3-31-2016

BSM