**IN THE UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF KENTUCKY**
**NORTHERN DIVISION**
**COVINGTON**

CRIMINAL CASE NO. 2:16-CR-47-ART

UNITED STATES OF AMERICA, PLAINTIFF,

v.

WILLIAM MILLER, DEFENDANT.

**DECLARATION OF JOHN SHEHAN**

I, JOHN SHEHAN, hereby state and declare as follows:

1. I am currently employed as Vice President of the Exploited Children Division ("ECD") at The National Center for Missing and Exploited Children ("NCMEC"). I have been employed by NCMEC since February 2000. As Vice President, I am responsible for supervising NCMEC's CyberTipline®. I am familiar with the operations of the CyberTipline, including the procedures involving the receipt and processing of reports by NCMEC and the procedures used to generate and maintain reports. The information contained in this declaration is based on my own personal knowledge and information to which I have access in my role as Vice President of ECD for NCMEC.

## I. NCMEC Background

2. NCMEC is a private, nonprofit corporation, incorporated under the laws of the District of Columbia. It was created to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC serves as the national clearinghouse for families, victims, private industry, law enforcement, and other professionals on information and programs related to missing and exploited children issues. NCMEC employs over 325 individuals and works with hundreds of volunteers to facilitate outreach and community child safety events nationwide.

3. Like other large nonprofits, NCMEC receives federal grant and private foundation funding, corporate financial and in-kind donations, and private individual donations to maintain and

enhance its 22 programs of work, including conducting community safety presentations, working with corporate and photo partners to disseminate posters of missing children, providing prevention resource materials and curricula to educators and schools, and engaging with parents, families, social service agencies, law enforcement, and schools on issues relating to missing and exploited children.

4. NCMEC receives millions of dollars in private funding and in-kind donations from corporations and individuals and works closely with its corporate partners to develop educational programs and materials to keep children safe. For instance, Disney sponsors NCMEC's Educator Online Training Program, a self-paced online training program to help schools teach Internet safety and good digital citizenship to children; Old Navy sponsors child ID and child safety informational events for its customers; and Honeywell sponsors KidSmartz®, a child safety program that educates families about preventing abduction and empowering children in grades K-5 to practice safer behaviors. NCMEC also works with over 250 corporate partners to disseminate photos of missing children to millions of homes across the United States each week.

## II. NCMEC's CyberTipline

5. NCMEC launched the CyberTipline on March 9, 1998, to serve as the national online clearinghouse for tips and leads about child sexual exploitation. The CyberTipline (www.missingkids.org/cybertipline) was developed to further NCMEC's mission of helping prevent and diminish the sexual exploitation of children by allowing the public and electronic service providers ("ESPs") to report online (and via toll-free telephone) the enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, misleading words or digital images on the Internet.

6. A secure CyberTipline was created in February 2000 to facilitate the reporting of apparent child pornography by ESPs. Once registered with NCMEC, ESPs can upload files relating to child sexual

exploitation content when making reports to NCMEC using a secure electronic connection. Uploaded image files may include images, video or other reported content.

7. Neither the government nor any law enforcement agency created the CyberTipline or has input into CyberTipline operations. The government does not instigate, direct or provide guidance to NCMEC in its processing of CyberTipline reports.

8. NCMEC began operating the CyberTipline before any federal legislation was enacted that referred to the CyberTipline. The infrastructure of the CyberTipline was built from a private corporate donation from Sun Microsystems, Inc. that included hardware, software, and programming.

9. NCMEC staff cannot alter or change information submitted by a reporting ESP. NCMEC does not direct or mandate the type of information that an ESP may choose to submit in a CyberTipline report, but instead provides voluntary reporting fields that ESPs may populate with information, including uploading apparent child pornography image files.

10. After an ESP makes a CyberTipline report to NCMEC, a staff member uses conventional and publicly-available open source tools to try to identify potential geographic information pertaining to the individual who is the subject of the report as well as geographic information of the ESP potentially used in connection with the reported image files.

11. NCMEC is required only to make CyberTipline reports available to law enforcement. NCMEC is not required to open reported image files or review any content provided by a member of the public or an ESP in a CyberTipline report. If NCMEC independently decides to open a reported image file or review the contents of a CyberTipline report, it does so pursuant to its internal organizational and operational guidelines and in furtherance of its private mission to aid children.

12. NCMEC does not open or view every image file submitted in a CyberTipline report. Pursuant to NCMEC's current review process, NCMEC staff make an independent determination whether to open reported image files based on operational factors, including but not limited to the volume of reports, whether a child might be in imminent danger, and the need to determine a potential geographic location of a child victim or reported user. As of February 4, 2017, NCMEC has received over 17 million

CyberTipline reports, including both international and domestic reports. Based on the volume of CyberTipline reports NCMEC receives, it is not possible to review all reports much less all image files.

13. After an ECD staff member has determined a potential geographic location and completed processing the CyberTipline report, the report is made available to a law enforcement agency in the potential geographic location for independent review and potential investigation. CyberTipline reports are made available to law enforcement in this way through the use of a secure virtual private network.

## III. CyberTipline Report 5778397

14. I have reviewed CyberTipline report 5778397 submitted to NCMEC by Google on July 10, 2015 in which Google reported an individual using an email address of "miller694u@gmail.com" with a reported login IP address of 74.132.31.22 and reported registration IP address of 74.139.62.188. Two (2) uploaded files are contained in CyberTipline report 5778397.

15. NCMEC staff did not open or view the two uploaded files contained in CyberTipline report 5778397 as indicated by the "Unconfirmed - Files not Reviewed by NCMEC" designation in Section C of the report. NCMEC staff queried publicly-available open source websites related to the "miller694u@gmail.com" email address reported by Google and located publicly-available social network profiles.

16. As indicated in Section B of CyberTipline report 5778397, NCMEC systems performed a publicly-available WhoIs lookup related to the 74.139.62.188 and 74.132.31.22 IP addresses reported by Google which appeared to be associated with a Time Warner Cable account having a potential geographic location of Ft. Mitchell, Kentucky.

17. CyberTipline report 5778397 was made available to the Kentucky State Police and the Kenton County Police Department for their independent review and potential investigation.

18. To the best of my knowledge, no law enforcement agency reviewed or processed CyberTipline report 5778397 prior to it being made available to law enforcement.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

DATED: Alexandria, Virginia, February 10, 2017.

JOHN SHEHAN

COMMONWEALTH OF VIRGINIA )
)
ALEXANDRIA CITY )

Signed and sworn to before me, a Notary Public, of City of Alexandria ~~County~~, Virginia, by John Shehan, on this 10th day of February, 2017.

SHERRY B. BAILEY NOTARY PUBLIC COMMONWEALTH OF VIRGINIA

Sherry B. Bailey

Notary Public

VA Notary Registration # 104859

My commission expires September 30, 2020