In the Matter of the Search of

# UNITED STATES DISTRICT COURT

for the

District of Massachusetts

(Briefly describe the property to be searched or identify the person by name and address)		) Case No. 15	5-mj-2245-MBB	a.
iPhone Model A1453 (IMEI) 35202706189436	53	)	, <u></u>	
AP	PLICATION FOR A	A SEARCH WAR	RANT	
I, a federal law enforcement of penalty of perjury that I have reason to property to be searched and give its location):	ficer or an attorney for believe that on the for	or the government, ollowing person or	request a search warrant a property (identify the person	and state under or describe the
Described in Attachment A				
located in the I person or describe the property to be seized):	District ofN	1assachusetts	, there is now conceal	ed (identify the
Described in Attachment B				
The basis for the search under evidence of a crime;			e):	
☐ contraband, fruits of contraband, fruits			ing a crime:	
☐ a person to be arrested				
The search is related to a violate	tion of:			
	Offense Description  Transportation of a Minor ini nterstate commerce to engage in prostitution or any sexual activity  Child Enticement			
The application is based on the				
See attached Affidavit of USPIS		Connelly		
		Commony		
☐ Continued on the attached☐ Delayed notice of dunder 18 U.S.C. § 3103a, t	ays (give exact endir	0	•	) is requested
		MICHAEL	Applicant's signature  GONNELLY, INSPECT	OR USPIS
Sworn to before me and signed in my p	presence.	17/3	181会编修	
Date: September 124	1,2015	Marier	Judge's signature	swler, USM
City and state: Boston, MA	=	US MAGE	STRATE MABIANNE B. E	BOWLER
			Printed name and title	

# AFFIDAVIT OF INSPECTOR MICHAEL J. CONNELLY IN SUPPORT OF A SEARCH WARRANT

- I, Michael J Connelly, being duly sworn, depose and state:
- I am an Inspector with the United States Postal 1. Inspection Service (USPIS) assigned to the Boston Division, in Boston, MA, having been so employed since 2007. As a Postal Inspector, I am responsible for the investigation of federal criminal offenses involving the transportation, distribution, receipt, and sale of child pornography through United States mail and related sexual offenses in violation of Title 18, United States Code, §§ 2252, 2252A, 2422, and 2423. I have completed the USPIS Basic Inspector Training (BIT) program in Potomac, MD and have conducted and assisted in numerous investigations of violations of state and federal laws involving child pornography and other child sexual exploitation offenses. I am also an affiliate member of the Massachusetts and Rhode Island Internet Crimes Against Children (ICAC) Taskforces and routinely work with agents, troopers, and officers with dozens of years of experience investigating crimes involving the sexual exploitation of children. I have received specialized training in the investigation of crimes involving the sexual exploitation of children by attending seminars and courses. I have investigated child pornography cases and related sexual offenses on a full-time basis since approximately May 2011.

2. The information contained in this affidavit is based on an investigation conducted by this affiant and information obtained by this affiant from other law enforcement agents involved in this investigation. In submitting this affidavit, I have not included each and every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause.

## IDENTIFICATION OF THE DEVICES TO BE EXAMINED

- 3. The property to be searched is a white and gold Apple iPhone, model #A1453, IMEI # 352027061894363, ("iPhone").
- 4. The iPhone is currently in the possession of the US

  Postal Inspection Service Boston Division and was obtained

  from a family member of the minor victim in this case,

  hereinafter referred to as "Minor A".
- 5. The warrant for which I am applying authorizes the forensic examination of iPhone for the purpose of identifying electronically stored data particularly described in Attachment B to this application and search warrant, which are items evidencing violations of:
  - a. 18 United States Code, § 2423(a), which makes it illegal for any person to knowingly transport an individual who has not attained the age of 18 years in interstate or foreign commerce, or in any commonwealth, territory or possession of the United States, with intent that the individual engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense.

b. 18 United States Code, § 2422(b), which makes it illegal for any person using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

#### PROBABLE CAUSE

- 6. On August 17, 2015, the Massachusetts Bay
  Transportation Authority ("MBTA") Transit Police received a
  request for assistance from a security guard at the South
  Station Bus Terminal in Boston, MA. The security guard reported
  observing suspicious activity between an adult male and a minor
  male including holding hands and touching each other under a
  blanket while inside the bus terminal.
- 7. Uniformed officers arrived on scene and separately questioned the two individuals they encountered at the bus terminal. One was identified as Jason M. Wolf ("Wolf"), DOB xx/xx/1985, who provided a Pennsylvania driver's license as proof of identification. The other individual ("Minor A") identified himself by name and stated that he was 15 years old.
- 8. During initial questioning law enforcement became suspicious as Wolf stated he met Minor A through the Big Brother Program. Minor A stated that they met through a mobile dating

application or app called Hornet<sup>1</sup>. Minor A also stated that they had taken a bus together from Maryland a few days earlier and recently arrived in Boston. Minor A stated that Wolf had provided the bus tickets for him. Minor A also stated that he and Wolf were leaving that day and taking a bus to Connecticut. Minor A also admitted to having oral and anal sexual intercourse with Wolf over the last few days in various locations including Maryland, Washington, D.C., New York, and Boston.

9. During questioning law enforcement observed Wolf take out his own iPhone and start going through the pictures and videos on the device. Wolf was then placed under arrest and transported to the MBTA Police Headquarters. Wolf was charged with aggravated statutory rape, in violation of MGL Ch. 265 §23, and enticement of a child for sex, in violation of MGL Ch. 265 § 26C. During Wolf's booking, law enforcement seized two bus tickets, an iPhone, the Motorola cell phone, a Toshiba external hard drive, a white USB thumb drive, and a black and blue "Urban Beats" digital music storage device. During booking, Wolf stated that the Motorola phone was not his and that it belonged to Minor A.

<sup>&</sup>lt;sup>1</sup> The following is taken from the website gthrnt.com which provides the mobile links to the Hornet application: "Hornet makes it fun and easy for gay, bi, and curious guys to meet each other. Find great dates and make new friends with this FREE gay app."

- 10. Wolf was advised of his rights and agreed to an interview. During the interview Wolf stated that he met Minor A on a dating site called Hornet and that he had communicated with Minor A via the Hornet app as well as another application called KIK<sup>2</sup>. Wolf went on to say he first met Minor A in person on or about July 10, 2015 in Maryland, he knew Minor A was 14 years old, and that their relationship was sexual. Wolf admitted to having oral and anal sex with Minor A in Maryland as well as engaging in mutual oral sex with Minor A while at their friends' residence in Roxbury, MA.
- 11. Officers also learned that Minor A was the subject of a missing person warrant out of Prince George's County,

  Maryland. Minor A was taken into protective custody and transported to an area hospital for evaluation.

#### VICTIM INTERVIEW

- 12. On August 19, 2015, a forensic interview of Minor A was conducted by a child forensic interviewer in Boston, MA.
- 13. Minor A stated he met Wolf online on or about July 9,
  2015 after receiving a message from him on the dating
  application Hornet. He began conversing with Wolf online via

<sup>&</sup>lt;sup>2</sup> Kik is a mobile texting/chatting application that advertises "Over 40% of American youth use Kik to chat, browse and share with their friends..."

iMessage<sup>3</sup> and the Hornet and met him in person the following day on July 10, 2015. The Hornet application is designed for mobile platforms and does not have a corresponding Internet website.

Minor A stated he used his own iPhone, (the subject of this search warrant,) which he had in Maryland, at the time to communicate with Wolf. Minor A stated he immediately began having a sexual relationship with Wolf. Minor A stated that he and Wolf had anal and oral sex in various locations in Washington, D.C., Maryland, New York, and in Boston.

- 14. During the interview Minor A stated that while in Maryland, the phone he used was a Gold Apple iPhone 5s which his uncle had originally got for him. Minor A stated that on or about July 9<sup>th</sup> he had gotten his phone back from his mother and it was when he first got his phone back that he first saw the message from Wolf on Hornet. Minor A stated that his phone was with his mother in Maryland.
- 15. Minor A stated that Wolf had purchased bus tickets for him and they travelled from Maryland to Boston. Minor A stated that Wolf had purchased bus tickets under false names for them. Minor A stated that Wolf had a laptop computer, but had sold it while they were in New York to obtain money to purchase bus tickets. Additionally, Minor A stated that he was using one of

<sup>&</sup>lt;sup>3</sup> iMessage is Apple's mobile messaging application which "lets you send messages back and forth with anyone on iPad, iPhone, iPod touch, or a Mac... Send photos, videos, locations, and contacts, too."

Wolf's old phones while traveling with him, which he described as a black Motorola cell phone.

- 16. During the interview, Minor A also stated that while in Annapolis, MD, Wolf used his iPhone to reserve a hotel room using the a mobile application called HotelTonight<sup>4</sup>. He also said that Wolf booked the hotel room under his own name and paid for it using his credit card. At the Annapolis Hotel, the victim stated that he and Wolf had oral sex and anal sex.
- another individual separately went on younow.com<sup>5</sup> from each of their phones, while in the same room. Minor A was using the black Motorola cell phone at the time and the three performed what is known as a "joint broadcast." During this "joint broadcast" on younow.com, the three individuals employed their phones to broadcast their live streaming video to other younow.com users.

<sup>&</sup>lt;sup>4</sup> HotelTonight is a mobile travel app for iPhone, iPad, Android and Windows devices that allows users to find discounted hotel accommodations up to seven days in advance throughout the Americas, Europe and Australia

<sup>&</sup>lt;sup>5</sup> Younow.com describes itself as "the best way to watch and broadcast interactive live stream videos. Discover talented broadcasters and chat live with people from around the world for free".

# REVIEW OF MINOR A'S ONLINE ACCOUNTS

- 18. Following the August 19, 2015 forensic interview of Minor A, law enforcement obtained Minor A's consent to view his various email and social media accounts by means of Minor A voluntarily providing his user names and associated passwords.
- 19. A review of Minor A's younow.com account identified over 100 video files which Minor A broadcasted to other younow.com users which were still available to view on his profile page. This affiant reviewed a sampling of approximately 30 of these videos, the vast majority of which depict Wolf on camera with Minor A. The videos vary in time from only a few seconds to several hours in length, and many of them depict Wolf being physically affectionate with Minor A including lying in bed with him, kissing him, and other manners of touching. In many of these videos, Wolf is seen holding a white apple iPhone.
- 20. Additionally, your affiant reviewed Minor A's

  Instagram<sup>6</sup> account, which contained numerous photographs posted

  since July 8' 2015. Several of the photographs are tagged by

  Minor A as depicting another user who Minor A identified as

  being Wolf. Additionally, one photo posted by Minor A depicts a

  table in a restaurant with numerous plates of food. The comments

<sup>&</sup>lt;sup>6</sup> Instagram is an online mobile photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, and share them on a variety of social networking platforms, such as Facebook, Twitter, Tumblr and Flickr.

state that Minor A is at Red Lobster with another user with a username known by law enforcement to be used by Wolf.

21. The Devices are currently the custody of USPIS Boston Division. In my training and experience, I know that the
Devices have been stored in a manner in which their contents
are, to the extent material to this investigation, in
substantially the same state as they were when the Devices first
came into the possession of law enforcement.

# AUGUST 25TH MEETING WITH MINOR A

22. On August 25, 2015, law enforcement met with Minor A with the permission of his attorney. During the meeting, Minor A voluntarily turned over the user IDs and passwords for some of his online social media accounts which law enforcement had previously been unable to access. Minor A also unlocked his iPhone and disabled the password and other security features. Without questioning or prompting, Minor A showed law enforcement his contacts on the iPhone and pointed out a contact listed as "My Forever" and identified it as Wolf's contact information.

# RECOVERY OF VICTIM iPHONE

23. On August 21, 2015, law enforcement went to Minor A's residence in a town in Maryland and spoke with Minor A's mother.

Minor A's mother voluntarily turned over a white and Gold Apple

iPhone, Model A1453, IMEI 352027061894363, to law enforcement and identified it as the phone belonging to and used by her son, Minor A.

# TECHNICAL TERMS

- 24. Based on my training and experience, I use the following technical terms to convey the following meanings:
  - Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can

also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as

names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

25. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs among other uses. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device, with whom the devices were used to communicate, and the content of certain electronic communications.

# ELECTRONIC STORAGE AND FORENSIC ANALYSIS

- 26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.
- 27. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:
  - a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
  - b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for

"indicia of occupancy" while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- 28. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for

would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire media, that might expose many parts of the Devices to human inspection in order to determine whether they are evidence described by the warrant.

29. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

# CONCLUSION

30. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Michael J Connelly US Postal Inspector

Sworn and subscribed before me this 16th day of September 2015.

MARIANNE B. BOWLER UNITED STATES MAGISTRATE JUDGE

# ATTACHMENT A

The property to be searched is:

A white and gold Apple iPhone, model #A1453, IMEI # 352027061894363, ("iPhone"

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

## ATTACHMENT B

- 1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2423(a), and 2422(b) and involving Wolf, Minor A, and other users believed to be minor children including:
  - a. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to the minor victim or her associated user account, email addresses, user IDs, or other identifiers associated with same.;
  - b. All notes, documents, records, correspondence, and address books, in any format or medium (including, but not limited to, digital data files or other electronic records) identifying other minors that Wolf may have been in contact with for the purposes of knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity, in violation of title 18, U.S.C. Section 2422(b).;
  - c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that pertain to accounts with any Internet Service Provider;

- d. Any records, documents, programs, applications, or materials that concern online storage or other remote computer storage;
- e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession and/or use of any digital device(s);
- f. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
- g. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- h. evidence of the attachment of other devices;
- i. passwords, encryption keys, and other access devices that may be necessary to access the device;

- j. records of or information about Internet Protocol
   addresses used by the device;
- 2. Evidence of user attribution showing who used or owned or used the Devices at the time the data described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and internet browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.