

Written Statement of

Patrick McNeil Beaver

Detective

Special Victims Unit

Loudoun County Sheriff's Office, Virginia

Northern Virginia/Washington D.C. Internet Crimes Against Children Task Force

Before the

House Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security,

and Investigations

Hearing on Combating Crimes Against Children: Assessing the Legal Landscape

March 16, 2017

Special Victim Investigations

Chairman Gowdy, Ranking Member Jackson Lee, and distinguished members, thank you for the opportunity to submit a written statement.

I'm Detective Patrick Beaver with the Loudoun County Sheriff's Office in the Commonwealth of Virginia. I have been assigned to the Special Victims Unit (SVU) and am currently assigned to the Northern Virginia/Washington, DC, Internet Crimes Against Children Task Force (NOVA/DC ICAC). In this capacity I have traveled all over the United States tracking down individuals who exploit children with cases originating in the Commonwealth of Virginia. While working cases involving the sexual exploitation of children, I have identified and rescued numerous children from sexually abusive situations. I'm also a computer forensic examiner certified in several forensic platforms for the identification of evidence to uncover the identity of an offender.

The Internet Crimes Against Children Task Force has been an essential partner for the Loudoun County Sheriff's Office and other agencies in the NOVA/DC region. The full support of ICAC has allowed our agency to combat child exploitation and the sexual abuse of children. The ICAC Task Force has provided specialized training opportunities for taskforce detectives to make them subject matter experts in special victim investigations. A detective's continued education is essential for providing services to victims and for arresting those who prey on juvenile victims through the exploitation of technology.

I have outlined below different challenges, successes, and recommendations for improvement in investigating Special Victims cases. The observations are from my experience and the experiences of the fellow detectives and agents with whom I work side by side every day to combat the sexual exploitation of children and hold accountable those who engage in these horrific crimes.

Overview of the Investigative Process:

In order to appropriately describe the legal landscape we encounter when combating crimes against children, it's appropriate to highlight how we encounter victims and work cases through the adjudication process.

Common report example:

A child victim is solicited online through social media to produce child pornography, exploited by an unknown suspect, and has sent several videos of child pornography to the suspect. The child victim has received threats to keep producing child pornography or the suspect will send the videos or pictures to the victim's friends/family.

Often we see victims exploited from the safety of their own homes while using their internet connected devices. In the past, if your children were at home, you knew they were safe from outside dangers like a sexual predator on the street or other criminal activity.

An investigation can begin one of several ways. For example, a victim residing in our jurisdiction can contact law enforcement to report a crime. A victim's family or other persons can also contact law enforcement to report the sexual exploitation of a child victim.

Detectives receive the case and seek consent from the victim's parent and the victim to conduct a forensic examination of the victim's electronic device. The in-depth forensic examination checks for any child exploitation material produced, distributed, and if any chats or suspect screen names exist on the victim's electronic device. We request all screen names associated with the victim and suspect as well as what social media or third party application was used.

A child forensic interview is usually conducted to obtain information from the child victim. The child forensic interview is conducted by a trained expert, either a fellow detective or child protective services (CPS) worker. The child forensic interview is almost always conducted at a Child Advocacy Center which plays an important role as a safe location and environment for a victim to disclose some of the most horrific incidents anyone could ever imagine. The Child Advocacy Center also offers services to the victim for continued assistance during this very fragile time in the young victim's life.

If the victim was sexually abused by the offender, the child would be referred to a local hospital that has a Forensic Assessment and Consultation Team. These services are essential for providing the victim with the appropriate examination to collect evidence of a crime and to provide medical care.

Once detectives identify the electronic service provider (ESP), they send necessary legal process (search warrant/subpoena) to the company requesting name, address, e-mail, and internet protocol (IP) connection logs and content associated with the exploitation of the child. This is where our investigation either accelerates or hits a brick wall depending on the company's willingness to accept, process, and respond in a timely manner to our legal process.

Should detectives receive valid investigative information from the company involved, detectives work to identify and arrest the suspect through a series of search warrants and interviews. Investigative steps vary in every case and this example is just one of many steps which can be used by a detective.

During the investigation, it's common to consult with the Commonwealth Attorney's Office or the Attorney General's Office of Virginia for guidance on charges and certain legal paperwork. This relationship with the prosecutor(s) is essential to bringing the case from an arrest to a conviction of a child sex predator.

I will outline below the challenges with ESPs and success we're having on getting a rapid response for legal returns in certain cases. Furthermore, I will outline challenges with charging juveniles with distribution of child pornography and when it's appropriate to charge a juvenile with respect to them being placed on the sex offender registry.

Evolution of Technology in Crimes Against Children:

The evolution of technology, and the wide use of the internet on multiple devices in a residence has had an unintended effect on the safety of our children in our communities. The launch of a third party application on a cell phone, computer, or tablet can open the doors to a residence to not just one child sex predator but an entire world of individuals looking to sexually exploit a child.

In investigations of child pornography and sexual exploitation of children, we see children being victimized for hours, days, months, and years at a time. In some cases, the suspect demands the juvenile leave their parent's presence to produce child pornography only to have the juvenile return to the dinner table frozen with no solutions or outlet to report these incidents due to the threats of distributing the victim's images or videos to his/her friends. We've seen children convinced to exit the safety of their home to meet their offender, allowing the offender to sexually abuse the child.

Child victims often have zero means of transportation outside of their parents. Detectives have observed the use of car service applications on phones to lure a child from their residence and be transported to the hands of the sexual predator. This alarming trend has increased significantly over the past two years. For example, the suspect sends a car service company car near the victim's residence and directs the child where to go. The child victim gets in the vehicle and the driver already knows where to go because the suspect has already provided this information. On many occasions, an interview of the car service driver reveals he/she had no idea what was taking place, felt something was wrong, but did not contact law enforcement.

Detectives have had great cooperation from car service application companies with legal requests but, in most cases, it's after the sexual assault and exploitation has already been committed, not before.

The sexual exploitation of a child can be as quick as one photo/video being sent but the continued exploitation of the victim lasts for years to come. In situations where the suspect has been arrested and placed in jail, the exploitation of the juvenile continues as the image/video travels from suspect to suspect and server to server worldwide.

Unfortunately, at times the image/video has GEO-Location data embedded in its metadata. A suspect with basic knowledge of metadata would thus be able to identify where the photo was taken. Often images and videos of the victims are produced inside the safety of their own residence but young victims may not even know their location data (GEO-Location) was turned on. This leaves the victim open to continuous threats by unknown sexual predators throughout the world, even after the original suspect is in jail.

Being a computer/cell phone forensic examiner has allowed me to observe changes in technology and certain trends by companies. I have observed the continued evolution of encryption and methods used by companies to preserve the privacy of their customer. In the attempt to preserve the privacy of the user, companies have created software/hardware resistant to certain law enforcement tools used to conduct a forensic examination of a victim's electronics and suspect's electronics. At times, even with a password and an "unlocked" device, a forensic examiner is unable to retrieve full data from the device due to certain barriers established by the manufacturer in a forensically sound way.

When discussing the evolution of technology in relation to crimes against children we should look at trends for the future of electronics. Recent examinations of electronic evidence is showing less

dependency on device storage data by the end user. I have observed an increased use of the "cloud" by suspects to store their data for little to no cost.

I have observed the encryption of data stored in the cloud through legal services. Select companies who store data purposely distance themselves from being able to decrypt the data when served with a search warrant. In the same respect, I'm encouraged by certain companies who proactively report child exploitation material on their servers. These companies turn the information over to law enforcement or other designee set by federal code and these reports are processed by the National Center for Missing and Exploited Children (NCMEC). Companies that hand over child exploitation hold a user agreement with the user of the account. The user of the account has agreed to the terms and conditions when signing up for an account.

Encryption has become very common for companies attempting to sell a secure devices or services to a consumer. I would submit that most devices these days have the ability to be encrypted without the consent or knowledge of the end user. It's a known fear of law enforcement that date encryption and storage of such material on the cloud will lock victims virtually in the cloud without hope of rescue. Certain metadata embedded in each photo or video could be a key element in solving a case of a child being exploited.

Over the past three years I have observed another trend by suspects to hide their identities through the Dark Web and Virtual Private Networks (VPN). A VPN will show a different IP address from the victim's or suspects true IP address. VPN's used to be a complex setup for the user requiring knowledge and access to a VPN. The use of VPN services has increased dramatically by victims and suspects in child exploitation cases.

Interviews of victims have shown the use of third party VPN services with literally one click of a button. Victims describe to me that VPNs allow them to access blocked content while utilizing the school's Wi-Fi. Unknown to the victim, this keeps law enforcement from being able to identify their IP address and, ultimately, finding the victim should they be exploited or abducted. The same goes for suspects who wish to hide their true identity. Suspects have always used new technology to mask their identity and hide from law enforcement. Later, I will describe the legal barriers set by VPN companies and potential solutions for compliance with legal process by law enforcement.

The above overview of technology's evolution in relation to crimes against children is the essential part of an investigation that will lead detectives to hold suspects accountable for their crimes. The examples describe everyday challenges to myself and my fellow detectives. One of the hardest things in my career is to tell a victim we could not find the individual who exploited them because a company has chosen to protect the "privacy" of a child sex offender in order to keep business.

Legal barriers in crimes against children: Detective perspective:

As a detective I encounter legal barriers from the beginning of an investigation to the conviction and, sometimes, the release of a suspect as a registered sex offender back to society. I will outline below the challenges we have observed in relation to legal process to companies serving as internet service providers (ISP) or electronic service providers (ESP). I will outline issues with companies outside of the boundaries of the United States from a local detective's perspective. Furthermore, I will outline issues with juvenile victims producing and possessing child exploitation material.

Legal response from companies:

As detectives investigate a case or go undercover to talk with a suspect there are many legal implications to be considered. One very important question is which company will have to be serve with legal

process? And, will they respond in a timely manner or hinder the investigation by notifying the suspect of my inquiry?

When a detective in the Commonwealth of Virginia obtains a search warrant on a foreign corporation ESP outside of Virginia they must send that legal paperwork to the company either via email or fax. The detective notifies the ESP when submitting the search warrant that the investigation is in reference to child exploitation. This paperwork to identify a suspect or obtain subscriber information is crucial to the detective's investigation of a child exploitation case.

Many times I submit legal process and immediately get notified by the ESP that they will notify the suspect (user) of the legal process and will allow the user to fight the existence of the search warrant and the content within the scope of the search. This response even comes back to me when we have a "Do not disclose" written into the search warrant or have it sealed by our circuit court judges. This response may come a day or two after legal process has been submitted. With some ESP's, however, it takes several emails over a period days to get the message conveyed to them.

The trend of ESP's to notify suspects of a search warrant or subpoena has directly impacted cases throughout the United States and hinders the detective's investigation of a child exploitation case. The notification of legal process allows a child predator to erase and discard any evidence needed to hold them accountable for the exploitation of a child.

If the ESP agrees not to notify the child predator, you will wait sometimes weeks to a month to receive the search warrant/subpoena return. During the delay of legal response by the ESP, the child predator can—and sometimes does—continue this behavior with other victims. It should be noted some ESP's consistently agree not to notify the suspect and get the search warrant returned to the detective as soon as possible. At times, these companies are located outside of the United States but honor our legal process

and provide the proper legal return with the information requested. Compliance with legal processes by companies within the United States is sometimes harder than with companies outside the United States.

As noted previously, hosted VPN applications have become a key tool for a child predator's to hide their identity by masking their IP address. Legal process has been an extreme challenge with the ESP VPN companies with little to no results. We may provide the date, time, time zone, IP address, and Port number used, and receive negative results from the VPN companies from legal process. Individuals utilizing VPN for criminal activity and the exploitation of children may be located anywhere in the United States but have their IP address show up at a "server building" at any location that houses these. At times the server buildings claim to not keep logs of the user's true IP address. While VPN's can be used for legally everyday on the internet, it should be noted this is an ever increasing challenge for law enforcement in tracking down suspects engaged in child exploitation.

Certain ESP's have notified law enforcement they can only provide a legal return on data that they store on servers in the United States and are not obligated by a search warrant to provide this information in a search warrant return. This response is becoming common with legal returns and again protects the child predator and hinders law enforcement in conducting a thorough investigation.

Combating Child Pornography with Juvenile Offenders "Sexting":

As a detective investigating child exploitation, a challenge we encounter is when two juveniles of the same age share sexually explicit photos with each other and each is in possession of child porn, better known as "sexting". The problem faced by detectives in the Commonwealth of Virginia and other states is a lack of guidelines on when to charge for this example or alternative punishments. A detective must ask the prosecutor in the case whether or not to charge them with production, distribution, and possession of child pornography and then hope the court doesn't make them register as a sex offender. Additionally, what is the threshold to charge a juvenile with the above listed crime?

Over the past several years, I answered questions from school resource officers and fellow detectives looking for guidance on a weekly bases. Like many states, Virginia lacks “sexting” laws or even legal opinions for guidance in such cases and several pieces of legislation have failed in recent years. In the absence of these, the answer depends on the severity of the circumstances, age difference, coercion, and was it distributed to a third party. I believe in most circumstances where it’s defined as “sexting” we take the following steps:

1. Notify parents and offer services
2. Isolate the images through forensic examination
3. Notify NCMEC
4. Submit to NCMEC Child Victim Identification Program
5. Educate the parents and juvenile of the dangers of “sexting”
6. Interview/notify juvenile if they engage in this behavior a second time they will be referred for criminal prosecution, and outline the severity of the charges.

While many more steps would be included in combating “sexting”, this six step process would be able to track future violations of state law and give the juvenile a second chance to be educated.

Violent Juvenile Sex Offenders

I have encountered violent juvenile sex offenders while working Special Victims cases. Listed below is a case example where a juvenile suspect was placed on the sex offender registry and reoffended after getting out of jail.

I worked a 2012 case in which a 16 year old male suspect left the rear of his residence and began to walk around on the bike trail. After following from behind for a period of time, the juvenile suspect approached two juvenile females, ages 14 and 12, walking to school. The juvenile suspect grabbed one by the neck and pushed them against a fence. The male suspect sexually assaulted both juvenile female

victims. Both juvenile females fought back scratching the male suspect on the neck, breaking free and running away. The juvenile suspect proceeded to go home and play on his Xbox until I arrived to talk to him. I observed marks on the suspect's neck and subsequently interviewed him at our SVU office. The suspect was read his Miranda rights and agreed to speak with about the incident. The suspect admitted to wanting to take them back to his home and "molest" them as well as wanting to push one them in front of a bus to inflict injury.

The suspect was arrested and charged with two counts of abduction with the intent to defile and two counts of aggravated sexual battery. The suspect pled guilty as a juvenile and was sent to jail. The suspect was also required to register as a sex offender.

The suspect was subsequently released from jail at the age of 19 and was allowed to reside at the same address where the bike trail was behind it. The suspect was allowed to work at several different places to include a restaurant while being monitored by GPS and a Virginia State Police Trooper.

In 2016 I received a phone call to respond to a sex offense where a suspect (same suspect from above) working as a restaurant dishwasher had sexually attacked two children, ages 7 and 8. The now-adult sex offender abducted two young children, sexually assaulted them inside a bathroom, and returned to washing dishes. The sex offender again was placed under arrest and agreed to speak with me.

The suspect admitted to this horrible crime. During my interview with the suspect I asked him if he should have been out of jail yet. The suspect advised he was surprised when they let him out of jail. The suspect noted he would go to sex shops and buy blowup dolls and had thought about sexually assaulting again. The suspect noted he had failed a polygraph and didn't tell his probation officer or his sex offender registry Trooper he was having these feelings. The suspect was sentenced in 2016 to life in prison with

all but 54 years suspended. Upon his release he will be evaluated for civil commitment as a sexually violent predator.

Take note of the offenses the suspect committed as a juvenile and the appropriate application of the use of the sex offender registry. It should be noted when sex offenders are released back into society they can still offend and sometimes commit even worse crimes against even younger victims. The location where the suspect worked placed him in contact with children and made it easy for him to attack the victims. Even with GPS monitoring and the best supervision of a sex offender, all they need is a moment to commit one of the most horrific crimes against a child.

Education:

The Loudoun County Sheriff's Office and the NOVA/DC ICAC Task Force conduct trainings to educate parents and children of the dangers of the internet and the exploitation of children.

The Loudoun County Sheriff's Office holds evening sessions for parents who want to be up to date on how to protect their family. The Sheriff's Office also teaches students how to protect themselves from online predators.

The Loudoun County Sheriff's Office hosts a Child Safety Day once a year to allow for families to meet SVU detectives and see the tools we use to keep their families safe. This program has been a great success with hundreds if not thousands of attendees each year.

Summary:

Working crimes against children cases has been the most rewarding thing I have done in my career. The ability to rescue a child and directly make a difference in my community keeps me going day to day. We face challenges ahead in the legal landscape in fighting crimes against children. Absolute oversight in the

legal process is needed to prevent child predators from being protected by companies who only wish to keep a customer. I fear the window is narrowing where technology will outstep our legal process. Victims will be left in the dark and sexual predators will have the upper hand in keeping their identities hidden from law enforcement.

Thank you for the opportunity to share this information with you today. I hope my narrative will be of use as you look further at this issue. Please do not hesitate to contact me with any questions.