**Statement of Captain Charles Cohen**

**Commander, Intelligence and Investigative Technologies**

**Indiana State Police**

**April 19, 2016**

**Hearing Before the Committee on Energy and Commerce**

**Subcommittee on Oversight and Investigations**

**United States House of Representatives**

**"Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"**

Chairman Murphy, Ranking Member DeGette, Members of the Subcommittee:

My name is Chuck Cohen and I am a Captain with the Indiana State Police, responsible for the Office of Intelligence and Investigative Technologies. I also serve as the Indiana Internet Crimes Against Children Task Force Commander and as the Executive Director of the Indiana Intelligence Fusion Center. I have conducted criminal investigations for 21 years. For over 15 years, those investigations have involved internet crimes against children. Internet crimes against children include the production, dissemination, and possession of child pornography, online child solicitation, and online child sexual extortion. While my testimony focuses on this narrow set of criminal activities, the implications are the same for any type of criminal investigation.

During my years as an investigator, I have not seen any impediment to rescuing child victims or identifying and prosecuting child sexual predators that even comes close to the impediment created by encryption. It is a fact that encryption prevents law enforcement from lawfully gathering evidence. Encryption is great if you are a private individual who wants to keep your tax information private, if you work at a doctor's office and need to keep patients' medical records safe, or if you own a business whose internal communications relate to the development of highly sensitive intellectual property. I get that, and so does everyone else in law enforcement. I want my information in my personal life to be secure from unauthorized access as much as the next person, but we must not allow ourselves to be blind to the relative harms.

Encryption is necessary, but it is also necessary for criminal investigators to have access to both stored data and data in transit when lawfully authorized.

Put yourselves in the shoes of the parents of a child whom we have just discovered is being victimized online. The victimizer has thousands of photographs of your child in a digital vault that is impossible for law enforcement to open. Your child's abuser has ready access to the

contraband, but can possess and disseminate it with impunity. Again, the fact is that encryption puts those images of child abuse beyond the reach of law enforcement. In this case, it is the depraved individual harming a child, not society, that benefits from encryption.

Encryption is not new. What *is* new over the last three years is encryption moving from something that people could seek out and deploy if they had the specific desire to conceal information or communication, to something that is being deployed by default into data storage systems including cell phones and hard disk drives, operating systems such as iOS and Android, and communications platforms such as WhatsApp and Viber. At the same time, the encryption has reached a level of technical and mathematical sophistication that often makes it impossible to defeat.

The march to encrypt everything means that more and more evidence at rest on devices and in motion across networks is unavailable to law enforcement by default, no matter what legal demands we obtain.

I have grave concerns that within the next several years, if nothing changes, we will substantially lose our ability to conduct Internet crimes against children investigations as a direct result of the ubiquity with which encryption is being built by default into devices, operating systems, and online communication systems.

Private companies in the United States and around the world have unilaterally decided, without checks and balances, to deploy unbreakable encryption in the most widely used communications devices and computing systems. This threatens to present an insurmountable challenge to local, state, and federal law enforcement conducting a wide variety of routine criminal investigations. Nowhere is this more evident than during the investigations of internet crimes against children since these crimes rely so heavily on technology. That challenge is compounded because of the absence of requirements in the United States for Electronic Communication Service providers and Remote Computing Service providers to retain business records or transactional information.

In much the same way that some countries are viewed both by criminals and law enforcement as safe havens for money laundering and concealing proceeds of unlawful activity due to weak legislation and a lack of regulation, I am concerned that the United States may become viewed as a safe haven for those who sexually exploit and victimize children.

As far as I know, the FBI is not exaggerating or trying to mislead anyone when they say that there is currently no way to recover data from newer iPhones. Data from the San Bernardino County iPhone was able to be accessed because it was an iPhone 5c with a 32-bit processor. iPhone models that are 5s or newer have 64-bit processors. Essentially, a faster processor can support more powerful encryption. I am aware of no current means available to law enforcement to defeat the encryption of 64-bit iPhones running iOS 8 or higher.

Apple has intentionally designed an operating system and device combination that functionally acts as a locked container without a key. The sensitivity of the personal information people keep stored in their phones should be compared to the sensitivity of information that people keep in bank deposit boxes and their bedrooms. While criminal investigators with proper legal authorization have the technical means to access both deposit boxes and bedrooms, we lack the technical means to access new cellular phones running default hard encryption.

Under normal conditions, when there is reason to extract data from a cell phone during a criminal investigation, the first (and usually only) step is to do both logical and physical memory extractions. There are several commercial and custom tools that aid both in the extraction and indexing of the extracted data.

When the phone's data port is destroyed, nonfunctional, the data is encrypted, or the phone has been damaged, the next step is to do a JTAG examination. JTAG stands for Joint Test Action Group. These are the solder points on the motherboard that are used by the manufacturer to test the firmware. So, the examiner solders leads to the JTAG points and uses that connection to extract the data from the memory chip. This method works on many phones. But, this method does not work for encrypted iPhones or phones using encrypted Android operating systems.

When JTAG is not an option, the next step is called an In-System Programming (ISP) examination. This is conducted after determining the location of small circuits on the phone's circuit board and micro soldering hair sized wires to the circuits under microscopic examination. This method also only works on non-encrypted devices.

The forensic method of last resort is a chip-off exam. To do this, a forensic examiner disassembles the phone, de-solders the memory chip from the motherboard, repairs the chip connectors if necessary, and reads the binary data from the chip. The examiner then runs the extracted binary data through software tools to index it. This method also does not work when the memory chip is encrypted.

The only other option we currently have is to attempt brute force methods to correctly guess the passcode. But if the user has set the iPhone to overwrite the data after ten failed password attempts, this method is not possible either.

Apple, as an example, deploys an unbeatable combination of hardware and software encryption on iPhone 5S and higher running iOS 8 and higher. This combination is not found on other cell phones and requires the pairing of the unique memory chip with the unique encryption chip in combination with the key to the software encryption in order to access data. I can think of two reasons why a cell phone or mobile operating system designer would want to do this: to reduce liability and cost by making themselves technically unable to help a government agency seeking assistance; or to outright prevent extraction of data during a forensic examination when someone has physical control of the device and is using advanced hardware and software forensic tools

I have heard some people on news programs and in testimony say that companies should not have to assist the government in trying to obtain evidence on a device because "the government must have some secret way of defeating the encryption."

The short answer is: we do not. I have also heard so-called “experts” say that law enforcement can get everything we need with metadata. The short answer is: we cannot. Asking a detective to use only the metadata to solve an online crime is the equivalent of asking a detective to process a crime scene by only looking at the street address on the outside of the house where a crime was committed. I would not be here today if I was not encountering serious problems that do not have easy technological fixes. We need help, and it is increasingly apparent that this help must be legislative.

We are often asked for examples of how encryption hinders law enforcement’s ability to conduct criminal investigations. There are numerous encrypted phones sitting in Indiana State Police evidence rooms waiting for a solution - legal or technical - to the problem. Some of those phones belong to murder victims and child sex crimes victims.

We have unfortunately reached a point where we now ask investigators for the phone type and operating system before we accept them for analysis in a case. In many instances, we need to tell the investigator that there is nothing that can be done to extract the data from newer 64-bit iPhones and encrypted Android operating system phones. While those phones sit, and while there is no solution, investigations go unsolved and victims go without justice. This challenge is exacerbated when combined with cloud storage encryption and encrypted communication. The bottom line is that we are left with fewer leads to investigate.

Earlier this year, a mother and adult son were shot to death inside their home in Indiana. Both victims had newer iPhones. I am confident that, if they were able, both would give consent for us to forensically examine their phones to help us find their killer(s). But, unfortunately, being deceased they are unable to give consent, and unfortunately for those of us trying to solve their murders, they chose to buy phones running encrypted operating systems. I need to emphasize that we are talking not just about suspects’ phones, but also victims’ phone; and not just about incriminating evidence, but also exculpatory evidence that cannot be recovered.

Of course we pursue all leads in any investigation, but as we push deeper into the technology and data era, an increasing percentage of the evidence that is critical to any case is in electronic storage somewhere—on a device, on electronic storage media, on a network, or in the cloud. If we cannot get it, then it is harder to generate leads and harder to solve crimes.

It is difficult to determine how many cell phones Indiana State Police forensic examiners are not able to examine due to encryption. That is because when certain combinations of devices and operating systems are encountered during an investigation, they are not even accepted for examination because investigators and examiners know they cannot defeat the encryption either technically or through the service of legal process.

What we do know is that in 2015 the Indiana State Police examined over 1,000 cell phones linked to crimes that were committed. Forensic examiners working for the Indiana State Police estimate that in excess of 40% of all cell phones encountered during the course of Internet crimes against children investigations have encryption that prohibits forensic examination. The requests received for forensic examinations that cannot be serviced due to encryption is constantly increasing. Over 80% of those phones that have been forensically examined during the course of Internet crimes against children investigations contain evidence of the sexual exploitation of children or child pornography. This means that there is a lot of evidence on a lot of phones sitting on our desks right now. And these are serial crimes: the offenders do it over and over again until they are caught. We absolutely know that we could stop pedophiles today if we had access to data on the encrypted phones sitting in our evidence rooms. But we're stuck, and children continue to be victimized.

Another example comes from Burlington County, New Jersey where police are working an active investigation into the manufacturing of child pornography. But police cannot access the data on an encrypted phone that is central to the investigation.

In Guilderland, New York, police have two iPhones that cannot be unlocked that they believe hold critical evidence in a quadruple murder case where four members of a family were killed.

Massachusetts State Police death investigators are overwhelmed with heroin overdoses right now. In several cases they have recovered locked phones which likely contain evidence regarding circumstances of death or the victim's drug supplier, but the data is unobtainable.

Also in Massachusetts, the State Police Computer Crimes Unit, which handles child pornography and physical child sexual exploitation investigations, are increasingly forced to note "phone locked and not examined" in their case reports.

These are a handful among thousands of cases around the country that are currently stymied by encrypted devices.In February 2016, Apple announced that it was going tie the encryption of iCloud accounts to the device encryption key. It is important to note since Apple currently stores the keys, it can currently comply with the proper service of a search warrant based on probable cause for the contents of an iCloud account. Transferring the key to the device means that Apple will no longer have the technical ability to comply with the proper service of legal process related to iCloud accounts. Moving the location of the encryption key, which Apple plans to do, is different from hardening firewalls, which Apple has not announced plans to do. Hardening firewalls provides additional safeguards from malicious intrusion for customers while still allowing Apple to comply with the proper service of a search warrant.

I have heard the question asked, "Can't the FBI just help state and local law enforcement when encrypted devices or communication is encountered?" The Indiana State Police has some of the most skilled forensic examiners and most advanced hardware and software tools to conduct forensic examinations of digital devices and electronic storage media. I am very familiar with the commercial and proprietary forensic tools available to law enforcement. I can

say definitively that there is no solution for recovering data from many encrypted devices and hard drives. And, I can also say definitively that there is no way to technically obtain the transactional information or communication content from many encrypted communications platforms such as Wickr, WhatsApp, Viber, Telegram, and Skype.

As more platforms, such as Gmail, Yahoo, and WhatsApp move to robust encryption by default, those who investigate Internet crimes against children are truly "going dark."

Unlike many other crimes and contact sex offenses against children, Internet crimes against children can be perpetrated completely online and obfuscated by hard encryption. But, make no mistake, these crimes are devastating to victims and victims' families in ways that are without parallel and are difficult to fully conceive unless you routinely interact with these victim populations. They are also incredibly difficult on law enforcement investigators who spend a significant portion of their time reviewing the evidence and interacting with the victims.

It is always difficult to know what evidence and contraband is not being recovered, the child victims that are not being rescued, and the child sex offenders that are not being arrested as the result of encryption. But the investigation, prosecution, and federal conviction of Randall R. Fletcher helps to shed light on the type of evidence being concealed by encryption.

Fletcher lived in Northern Indiana. During the course of an investigation in 2009 for production and possession of child pornography, a computer hard drive with an encrypted partition was seized, along with a separate encrypted hard drive and an encrypted thumb drive. The encryption was robust such that it was not possible to forensically examine the encrypted data. A federal judge compelled Fletcher to disclose his encryption key. Fletcher initially denied remembering the key but failed a polygraph examination on that question. He then provided law enforcement with a passcode that was found to open two of the encrypted containers – the encrypted partition and the additional hard drive – but which did not open the encrypted thumb drive. In the newly opened data, law enforcement found thousands of images and videos depicting minors being caused to engage in sexually explicit conduct. Fletcher denied that the thumb drive contained encryption, but his own computer forensic expert disagreed. To date, all efforts to technically break the encryption on the USB storage device have failed. And, to this day, investigators believe that the thumb drive contains homemade child pornography produced by Fletcher, but have no way of confirming or disproving that belief. Fletcher had continuing and ongoing access to children, including a child he had previously photographed in lascivious poses.

In 1995, Fletcher was convicted of conspiracy to commit murder after he hatched a plan to shoot and kill the mother his then-15-year-old girlfriend. Seven years later, in 2004, while still on probation, Fletcher was found to be in possession of images and videos featuring minor children. By the time he was investigated again in 2009, Fletcher had downloaded encryption software and set about attempting to hide his massive collection containing thousands of child pornography images and videos from law enforcement.

Fletcher is currently serving a 30-year term of imprisonment in a federal facility, to be followed by lifetime supervised release. The encryption used by Fletcher withstood numerous examination attempts and forensic techniques attempted by several law enforcement agencies. There is good reason to believe and it is quite possible that, because of hard encryption on the USB storage device, additional crimes committed by Fletcher have not been investigated and prosecuted and additional child victims have not been provided victim services or access to the justice they so richly deserve.

Unless Congress acts soon to require compliance with a warrant, I anticipate that the choices being made today by technology companies to rapidly move to ubiquitous hard encryption will cripple investigations into the most disgusting of crimes - Internet crimes against children.

The Fourth Amendment protects people "…against unreasonable searches and seizures…" by the government, not against all searches and seizures. Since the founding of the country, if I received a warrant, issued by an impartial judge or magistrate, based on oath or affirmation, specifically describing the place to be searched, and the items authorized to be seized, as a police officer I could serve that warrant. It does not matter how well the residence or business was locked or how strong the safe is, I can gain access. Now, for the first time in the history of the United States, private companies located in the United States and elsewhere are making business decisions, without oversight or checks and balances, to create virtual safes and strong boxes that cannot be opened.

These companies have made unilateral decisions to reach beyond the protections of the 4th Amendment and place evidence of crimes, including child sex offenses, beyond not just unreasonable searches, but against all searches. And, this is clearly a business decision rather than one based on concerns about privacy or civil liberties because it has widely been reported in the media that when certain countries other than the United States require modifications to operating systems, revelation of source code, or modifications to communications platforms, the same companies make certain modifications in order to do business in those countries.

Several factors are working together to create "the perfect storm" such that those who conduct investigations involving child pornography, online child solicitation, and online child sexual extortion are "going dark". Those factors are - in order of impact:

1. data and communication encryption,
2. no U.S. federal law setting retention periods for Electronic Communication Service providers or Remote Computing Service providers,
3. the ability for sexual predators to engage in criminal communication facilitated by companies that are not required to comply with the service of U.S. legal process; and,
4. the unwillingness of service providers to comply with exigent circumstance requests when there is a child at imminent risk, often combined with the

notification of customer suspects when service providers are contacted by law enforcement to make such requests.

I hope that Congress takes the time to truly understand what is at stake with the "going dark" phenomenon and what problems are being created. In particular, please weigh the harms that an encryption scheme that allowed lawful access, even at the cost of some theoretically higher chance of lost data, against the very real human cost in failed investigations that we see across the country.

In my daily work, I feel the impact of law enforcement going dark. For me, it is a strong feeling of frustration because it makes the detectives and forensic examiners for whom I am responsible less effective. But for crime victims and their families, it is altogether different: it is infuriating, unfair, and incomprehensible why such critical information for solving crimes should be allowed to be completely out of reach.

I strongly encourage the committee members to contact your state investigative agency or local police department and ask about this challenge. I greatly appreciate your invitation to share my perspective and am happy to answer questions today or at any point in the future.