Major Cities Chiefs Association
Major County Sheriffs' Association

MAJOR COUNTY SHERIFFS

Achieving a Balance

Device Encryption, Privacy and Protecting the Public

With the advent of new encryption methods for communications devices, American Law Enforcement is rapidly losing the capability to lawfully obtain information necessary to protect the public from crime and violence. Moreover, advocates for enhanced privacy now seek to impose further barriers and restrictions that prevent law enforcement from obtaining historically lawfully accessible information, even when it's needed to stop violent criminals and to save lives.

The balance between public safety and privacy has tilted so far toward encryption that law enforcement leaders are compelled to speak out for crime victims and the public we are sworn to protect.

Encryption and Privacy

Law enforcement leaders embrace encryption and respect privacy rights. Police agencies have themselves been the victim of unlawful intrusions, cyber-attacks and the theft of sensitive data. To protect privacy and unreasonable searches, police are trained to follow strict procedures and required by law to obtain court orders when obtaining evidence that is protected. These established laws and procedures have served Americans well, and represent the balance between individual rights and protection of the public.

New measures designed to safeguard data security and privacy have thrown off the balance and have had an unintended result – they prevent local emergency responders from helping persons in danger and apprehending subjects who pose a threat to the public we serve. Both encryption technologies and proposed privacy measures have crossed over the point of balance and go to such extremes that police and sheriffs are prevented from discharging our most fundamental duty – protection of the public.

When police and sheriffs have a court approved warrant or there is an immediate threat of grave harm, service providers should respond with urgency, but that is not the reality we now face. Until the recent refusal by Apple to assist the FBI with a phone recovered by the San Bernardino terrorists, the public did not realize that police routinely face delay and roadblocks when attempting to obtain information from service providers and cellular device manufacturers – even when that information is needed to save lives and has been directed to be provided through a court order.

Is Technology Above the Law?

When lives are in danger and violent offenders seek to prey upon the public, industry should not be permitted to ignore court orders – no entity is above the law and no business model purposefully crafted to thwart criminal investigations should be lauded. Without action by Congress, these conditions will continue:

- ***Public Safety Emergencies***: encryption prevents police and rescue personnel from finding a missing person, a lost hiker, an Alzheimer's patient, or a heart attack victim.

- ***Criminal Investigations:*** encryption blocks law enforcement from finding an abducted child, apprehending a murderer, stopping a drug trafficker, or locating victims of human trafficking.

Manufacturers Defy the Courts

The defiance of lawful court orders is not due to encryption technology. Even before Apple refused to assist the FBI with the locked phone used by the San Bernardino terrorists, it was corporate policy to defy court orders. In a previous drug trafficking case where the U.S. Department of Justice served a Court order on Apple, the company openly admitted that the iPhone 5S running iOS 7 was not encrypted and the data may be extracted. But Apple has refused anyway, citing advertising concerns. In their brief filed in U.S. District Court, Apple said assisting law enforcement to apprehend the conspirators named in the warrant would ***"…tarnish the Apple brand."***[1]

NYPD Commissioner Bratton Describes Threat to New York

Following the attacks in Paris, NYPD Commissioner Bill Bratton spoke out about the importance to New York and the Nation. Speaking on ABC's ***This Week,*** the Commissioner of the Nation's largest police agency described why law enforcement must have access to phones in order to protect the public. When interviewed on CBS's ***Face the Nation,*** Bratton underscored the gravity of conditions when he said…

"We, in many respects, have gone blind…."

[1] Court Filing on behalf of Apple; Ken Dreifach: https://www.documentcloud.org/documents/2465705-apple-brief-10192015.html

Protecting Public Safety - Not Collecting Intelligence

The public reaction to revelations about Government surveillance and intercept programs has spilled over into public safety. Police do, and must be able to lawfully obtain digital information to save lives and stop crime – these are not Government intrusions.

- ***NOT - Intelligence Agencies of the Federal Government:*** Practices of intelligence agencies provoked controversy. Reactions to those programs should not be extended to law enforcement agencies with differing roles and responsibilities.

- ***NOT - Bulk Intercept and Surveillance:*** Mass email intercept operations are not conducted by law enforcement. Each instance has a warrant where Courts have authorized access to data in criminal investigations focused on individual suspects.

Emerging encryption capabilities and proposed privacy restrictions are reactions to revelations about practices by national security agencies, but new technologies and proposed privacy measures unintentionally or otherwise, block law enforcement from accessing historically and legally available information necessary to protecting the public.

How Encryption Can Threaten Public Safety

Police and Sheriffs have reported many real cases where encryption and privacy barriers have been misguided and harmful. This report documents cases where local law enforcement agencies have been unable to save lives and apprehend dangerous criminals due to technology and privacy obstacles that have thwarted lawful requests for information. (See Appendix A)

Law enforcement leaders do not seek legislation that goes beyond the established case law which protects privacy and individual rights. Proposed legislative measures would restore and maintain lawful access to data only when there is an urgent, critical need. Unless Congress acts to protect the public, these cases will become more widespread. Industry will continue to defy the law and refuse to assist law enforcement.

Police Need Digital Access to Protect the Public

The public does not realize how often police turn to digital technology to locate both victims and criminals. Whether to find a lost camper or a kidnap victim, police rely upon carriers to provide location data. When police have lawful access to digital cell phones, unencrypted information will lead rescuers to persons in danger and to the criminals who would do them harm.

When Encryption and Privacy Threaten Public Safety

The Kelsey Smith Case

When Kelsey Smith was abducted from a Target parking lot in Kansas, law enforcement agencies immediately requested location data from her cell phone carrier. Both her family and law enforcement agencies knew every minute was critical to finding Kelsey Smith alive and safe from harm. Despite the gravity of this abduction, the service provider took four days to respond - due to privacy concerns. Kelsey Smith was found dead less than an hour after law enforcement received her location information from the service provider. She had been raped and strangled to death with her own belt.[2]

The Brittney Mills Case

Baton Rouge mother Brittney Mills was eight months pregnant when she answered her front door. An avid fan of Apple, she had a diary, recipes and countless messages on her iPhone. She was shot to death on her front porch, where police found her iPhone. Her unborn son was delivered, but died a week later. Apple has said they could not pull anything off the encrypted device, with or without a warrant. Brittney's mother said to the press, "When something as horrible as this happens to a person, there should be no roadblock in the way for law enforcement to get in there and catch the person as quickly as possible."[3]

Garland, Texas Shooting

James B. Comey, the FBI Director, told senators that one of the attackers in a recent shooting in Garland, Texas "exchanged 109 messages with an overseas terrorist" the morning of the shooting that investigators could not read because they were encrypted. Without lawful access to these messages law enforcement cannot prevent or investigate threats. The shooting involved two men opening fire near an exhibit that showed cartoon images of the Prophet Muhammad. Police killed the attackers and the Islamic State claimed responsibility.

[2] http://www.foxnews.com/politics/2013/04/13/mother-murdered-teen-pushes-for-law-mandating-cell-phone-carriers-to-release/

[3] Encrypted Evidence is increasingly hampering criminal investigations (11/4) FULL TEXT

MAJOR COUNTY SHERIFFS

With Lawful Access, Police Save Lives and Serve Justice

Kidnapping Victim Found Alive

A woman was forcibly kidnapped from the driveway of her home on September 29, 2010, before law enforcement lost lawful access to encrypted phones. Her son received text messages and phone calls demanding money for her return. The cell phone that made the calls to the son was lawfully traced (by the Houston Police Department) which provided information associated to a residence. A vehicle that pulled out of the house was stopped and a person jumped out of the car and started running. Police pursued and ultimately arrested the suspect. The kidnapped woman was found after being bound and threatened, but she was found alive. This case was a success thanks to the lawful access to the cell phone that was still available to law enforcement before the increased encryption.

Justice for Six-Year-Old Victim

In 2014, The Houston Police Department (HPD) Special Victims Division Detectives utilized "passcode cracking" technology on an older model iPhone to find information needed to bring justice to a 6-year-old female victim. The iPhone contained images and videos of the suspect sexually abusing the victim. The suspect in this case received a sentence of 60 years on a charge of sexual performance by a child and 30 years on a charge of continuous sexual abuse of a child. The passcode cracking software was only used after a signed court order was obtained and can only be used on certain models of phones that do not have the higher level of security measures.

Recent events at home and abroad have underscored the urgent need to provide lawful access to cell phone data in terrorist cases. While the Garland case shows how the FBI was blocked from recovering vital information, the recent attacks in Paris and San Bernardino show how lives can be saved when police have lawful access during an emergency.

Access to Cell Phones in Terrorist Cases

San Bernardino Mass Shooting - Apple Refusal to Help Police

While the specifics of the San Bernardino shootings are still being investigated, it is already clear that information from the cell phones of the shooters is vital to a complete and thorough investigation. Syed Farook had photos of a public high school on one of the phones, which enabled law enforcement to sweep all of the schools he visited, a measure only possible because the data on his phone was unencrypted. In February 2016, FBI Director Comey testified that the FBI was unable to recover the encrypted information. When served with a Federal Court order to assist the FBI, Apple refused to comply.

Paris Attacks – Vital Information Recovered from Phones

The encrypted communications applications used for preplanning and coordination among the Paris attackers may have prevented the advance detection of the attacks, but the cell phone of one of the terrorists recovered outside the Bataclan theater helped investigators apprehend the ringleader of the attack, Abdelhamid Abaaoud. The phone was a model that was not encrypted and investigators found a text message sent, "let's go, we're starting," to indicate the start of the attack. When police identified Abaaoud's cousin in the phone's contacts list and her location in Paris, Abaaoud was located and police raided the apartment and thus stopped further terrorist attacks. It was later confirmed that Abaaoud died in the detonation of a suicide bomb during the raid.

Current Technological Barriers

Public safety would be well served by measures to facilitate, not hinder, law enforcement requests for assistance from service providers and manufacturers. Strong leadership will be required to adopt thoughtful policies and legislation in today's political climate. Congress must consider reasonable measures to protect the public, not bills that would further hamper public safety officials and the Courts.

In the aftermath of the Kelsey Smith tragedy, many States enacted legislation to require timely compliance with a police request for assistance, but Congress has yet to take any action to provide lawful access for law enforcement.

The scenarios below demonstrate the common encryption challenges for public safety in a variety of technologies:

- **Voice:** Detectives present a signed court order to intercept calls between persons engaged in human trafficking. Trying to find where the victims are to be taken and held, detectives cannot learn anything because voice communications are encrypted on the devices used by the cartel. Even when detectives recover phones during an arrest, the encrypted data cannot be recovered.
- **Text Messages:** Domestic terrorists are under surveillance by a local task force and have disclosed to undercover agents that they intend to commit violent crimes. Court authorized intercepts of unencrypted communications confirm that an attack has been planned, but even with a warrant, investigators cannot intercept their encrypted text messages and the attack goes forward.
- **Email:** Investigators have a warrant for email from a child pornography suspect - a previously convicted pedophile. When police try to read the email to his next victim, it is encrypted and they cannot respond before he has lured the victim to a planned meeting place.

Current Non-technological Barriers to Access

In addition to technological barriers to access such as encryption, law enforcement remains hampered by non-technological barriers to access due to a lack of service provider compliance standards. At a time when the Nation expects measures to provide for public safety, these conditions continue to worsen:

- **No Federal Compliance Requirements:** Neither Congress nor the FCC have imposed a mandatory requirement upon carriers to comply with law enforcement requests, even when lives are in danger**.**
- **No Penalties for Failure to Comply:** When providers refuse to obey a lawful request for assistance, including a warrant, there is no Federal penalty or remedy.
- **No Consistent Procedures or Policies:** The Federal Government has failed to establish a standard submission system for law enforcement to serve warrants and process on common carriers and internet service providers**.**
- **No Emergency or Exigent Provisions:** While courts have held that police need not obtain a search warrant when exigent circumstances demand immediate police actions, advocates would require a warrant in all cases, without regard to emergency conditions.
- **No Evidence Procedures:** Lacking any standards or legal requirements, carriers often damage the chain of custody and integrity of evidence.

- **No Retention Requirements:** There are no standardized retention schedules for digital information. Critical evidence may not be there when law enforcement needs it most to ensure justice and public safety.
- **Federal Law is Outdated:** Existing legislation is 20 years old and outdated by new technologies. Worse yet, it does not even apply to manufacturers.
- **No Required Technology Standards for Public Safety Access:** There are no technology standards that require "key enabled" entry for public safety to access critical information in the event of an emergency and with a court order.

Criminals Praise Apple for Helping

Rikers Island Prisoner: "Gift from God"

A Rikers Island prisoner in New York, in a recent taped conversation with an accomplice, illustrates a criminal's knowledge of the benefits encryption on the Apple iPhone with i0S8 or later.

"If our phones are running on the iO8 software, they can't open my phone," the inmate said. "That might be another gift from God."

Justice for Victims

"Going Dark" means that crime victims will be further harmed. Digital data represents the evidence of crimes - to which victims have a right.

- Victims of human/sex trafficking, of child exploitation, and other offenses where photographs and communications content are required – will be unable to get justice when key evidence is beyond the reach of the court.
- Child predators and other criminals who document their horrific crimes will be able to use encryption to their advantage. Without lawful access for law enforcement, key evidence will be hidden.
- The current voluntary response posture allowed for service providers permits destruction of evidence while law enforcement waits for release of the data.

Excessive Safeguards Also Hamper Criminal Defense

The discovery process in criminal cases requires all exculpatory evidence to be released by law enforcement and prosecutors. With full disk encryption, neither investigators nor the accused will be able to see or read what may exonerate the defendant.

- If manufacturers do not have keys to decrypt data, defendants will be unable to use communications content in their defense.
- If text messages are not retained by service providers, defendants cannot subpoena the content for their own defense.

Manhattan DA Unable to Execute 111 Warrants in a Year Due to Encryption

In a report released in November 2015, the Manhattan District Attorney's office compiled information on the impact encryption is having across its case load. The 111 warrants that were unable to be served due to the device or application being encrypted related to homicide, attempted murder, sexual abuse of minors, sex trafficking, assault, and robbery are just during the time period between September 17, 2014 and October 1, 2015. The report also covers how digital evidence was critical to similar cases. The report can be found here.

The Way Forward

Misguided privacy and encryption advocates now champion harmful technology that blocks law enforcement from protecting the public. Whether encryption or new privacy laws, we must oppose measures that threaten the public we are sworn to protect.

"Are we so mistrustful of government -- and of law enforcement -- that we are willing to let bad guys walk away, willing to leave victims in search of justice?" **James Comey, FBI Director. October 16, 2014**

The Director of the FBI has publicly called for reasonable measures that preserve the ability of law enforcement to protect the public. State and local law enforcement officials have joined the FBI to call for legislation that requires industry to comply with lawful requests to recover data that is essential for protection of the public from harm- the most fundamental duty of government.

Legislation: Protection of the Public Requires Immediate Action by Congress

Even industry giants must obey the law and comply with court orders. Congress must now take steps to clarify how and when law enforcement agencies may lawfully recover information form electronic devices, without reliance upon the All Writs Act of 1789. Both the Courts and industry have noted that there is no current legislation in place, and now question whether the All Writs Act should be applied to the latest technologies. Congress should end to the current debate by adopting clear and current legislation to protect the public, while respecting both privacy rights and proprietary technology.

The draft legislation proposed by Senators Feinstein and Burr would merely require service providers and manufacturers to comply with lawful requests from law enforcement and the Courts. It is time for Congress to legislate for the protection of victims and the public, and bring an end to the defiance that only protects criminals and terrorists.

Appendix A: Real-World Case Studies

The 30 real-world cases studies provided in this appendix include a sampling of successes that have been made possible through law enforcement's lawful access to devices and information; and failures that are as a result of law enforcement's inability to gain lawful access to information because of increased encryption and a lack of response to lawfully obtained court orders.

Cases Featured Above

These featured cases appear in this white paper for a complete reference of real-world case studies.

Case 1: The Kelsey Smith Case

When Kelsey Smith was abducted from a Target parking lot in Kansas, law enforcement agencies immediately requested location data from her cell phone carrier. Both her family and law enforcement agencies knew every minute was critical to finding Kelsey Smith alive and safe from harm. Despite the gravity of this abduction, the service provider took four days to respond - due to privacy concerns. Kelsey Smith was found dead less than an hour after law enforcement received her location information from the service provider. She had been raped and strangled to death with her own belt.

Case 2: The Brittney Mills Case

Baton Rouge mother Brittney Mills was eight months pregnant when she answered her front door. An avid fan of Apple, she had a diary, recipes and countless messages on her iPhone. She was shot to death on her front porch, where police found her iPhone. Her unborn son was delivered but died a week later. But Apple said they could not pull anything off the encrypted device, with or without a warrant. Brittney's mother said to the press, "When something as horrible as this happens to a person, there should be no roadblock in the way for law enforcement to get in there and catch the person as quickly as possible."[2]

Case 3: Garland, Texas Shooting

James B. Comey, the FBI Director, told senators that one of the attackers in a recent shooting in Garland, Texas "exchanged 109 messages with an overseas terrorist" the morning of the shooting that investigators could not read because they were encrypted. Without lawful access to these messages law enforcement cannot prevent or investigate threats. The shooting involved two men opening fire near an exhibit that showed cartoon images of the Prophet Muhammad. Police killed the attackers and the Islamic State claimed responsibility.

Case 4: Kidnapping Victim Found Alive

A woman was forcibly kidnapped from the driveway of her home on September 29, 2010, before law enforcement lost lawful access to encrypted phones. Her son received text messages and phone calls demanding money for her return. The cell phone that made the calls

to the son was lawfully traced which provided information associated to a residence. A vehicle that pulled out of the house was stopped and a person jumped out of the car and started running. Police pursued and ultimately arrested the suspect. The kidnapped woman was found after being bound and threatened, but she was found alive. This case was a success thanks to the lawful access to the cell phone that was still available to law enforcement before the increased encryption.

Case 5: Justice for Six-Year-Old Victim

In 2014, the HPD Special Victims Division Detectives utilized "passcode cracking" technology on an older model iPhone to find information needed to bring justice to a 6-year-old female victim. The iPhone contained images and videos of the suspect sexually abusing the victim. The suspect in thr case received a sentence of 60 years on a charge of sexual performance by a child and 30 years on a charge of continuous sexual abuse of a child. The passcode cracking software was only used after a signed court order was obtained and can only be used on certain models of phones that do not have the higher level of security measures.

Case 6: Paris Attacks

The encrypted communications applications used for preplanning and coordination among the Paris attackers may have prevented the advance detection of the attacks, but the cell phone of one of the terrorists recovered outside the Bataclan theater helped investigators apprehend the ringleader of the attack, Abdelhamid Abaaoud. The phone was a model that was not encrypted, so investigators found a text message sent, "let's go, we're starting," to indicate the start of the attack. Perhaps of greatest importance was the identification of Abaaoud's cousin in the phone's contacts list and her location in Paris where Abaaoud was ultimately located in a midnight raid and was confirmed to have died in a detonation of a suicide bomb at the time of the raid.

Case 7: San Bernardino Mass Shooting

While the specifics of the San Bernardino shootings are still being investigated, it is already clear that information from the cell phones of the shooters are providing vital clues. Syed Farook had photos of Carter High School in the San Bernardino area. Farook made regular visits to schools in the San Bernardino area and phots were recovered from his phone. On the day of the shootings, law enforcement did sweeps through all of the schools he visited, measures only possible because the data on his phone was unencrypted.

Case 8: Locked iPhone Impedes Murder Investigation

On Sunday March 1, 2015 Columbus Police responded to a report of a stabbing in the area of Summit Street and Northwood Avenue. Upon arrival, officers found the victim, lying critically injured. The victim was transported to The Ohio State University Hospital where he was pronounced dead at approximately 4:08 a.m. During the course of the investigation, detectives

developed information regarding a suspect and his whereabouts, and were told the suspect may have filmed or photographed the events just prior to the homicide using his cell phone. Detectives executed a search warrant on the suspect's home and placed him under arrest. During a search of the home, suspects recovered a locked iPhone 4S running iOS 8.1.2. As a result, detectives were unable to recover the potential evidence from the phone.

Case 9: Locked iPhone Blocks Murder Investigation

On Wednesday, October 29, 2014 Columbus Police were dispatched to a possible shooting. Responding officers located the victim lying in the street in front of the location. The victim sustained several gunshots to his upper body and was pronounced dead at the scene at 9:33 p.m. The investigation revealed the victim was working as a pizza delivery driver and was making a delivery at the time of his murder. Robbery appeared to be the motive for the crime and a search warrant was executed on one of the home of one of the suspects. The search resulted in the recovery of multiple cell phones, including a locked iPhone 4S running iOS 8.1.2. After conducting interviews with witnesses, detectives learned the crime may have been filmed by one of the suspects using his cell phone. Due to the iOS 8.1.2 software on the locked 4S, detectives were unable to recover the potential evidence from the phone.

Case 10: Delayed Response During Threat to Additional Victims

On July 30, 2015 Columbus Police officers responded to a report of a vehicle that crashed into a telephone pole. Officers arrived on scene and they located the victim who had been shot in the chest and died as a result of his injuries. It was determined the victim was in the process of delivering pizzas at the time of his death. Delivery receipts located in the victim's car showed the victim was delivering a pizza to a vacant house near the location of his death.

During the course of the investigation, a cell phone number was identified for the intended recipient of the pizza delivery, and it was determined the number was registered to a texting application that was downloaded to the phone. The application developer was contacted via an exigent circumstances request for subscriber information. They immediately complied and gave subscriber information, an email address, a phone ID to one of the pizza customers. The tech company was then contacted and an exigent circumstances request was submitted due to information that indicated the suspect had targeted a second pizza company prior to the murder, demonstrating the threat for further violent crime. The tech company refused to cooperate and stalled the investigation for several days because they did not believe an emergency existed.

A signed subpoena was secured from the Court, but the tech company indicated that was not enough to release the expanded subscriber information. The following day detectives got a court order signed by a common pleas judge, which the police submitted to the tech company (within an hour of being signed). Several days and multiple phone calls passed before the tech company eventually sent the information to detectives. The tech company provided the

detectives with several valuable pieces of information (e.g., real phone number, subscriber information).

Based on the information the detective received from the tech company, the detective issued an expedited court order to the cellular service provider, to start a live ping on the phone to get the phone location records from the night of the homicide. The detectives encountered the same resistance from the cellular provider as from the tech company. The cellular provider refused to ping the phone because it did not feel there was enough in the probable cause statement, despite it being signed by a judge. It took another several days before they finally sent the records to the detectives.

Case 11: Controlled Dangerous Substance (CDS) Distribution Investigation Hampered by Viber and iMessage

During a recent high-level/major offender CDS distribution investigation, investigators determined that the suspects were utilizing iMessage (iPhone data-based messaging) and Viber (third-party chat application) to communicate about CDS distribution activity. Though investigators had a court order and were authorized to intercept voice content and text message content, investigators were unable to do so with iMessage and Viber. Intercepted text messages from the suspects specifically instructed targets of the investigation to use Viber to share meet locations and conduct chats so they would not be accessible by law enforcement.

Viber is based outside of the U.S. in Cyprus, so investigators were unable to establish a lawful means to intercept of communications that occurred on Viber. iMessage is an Apple product and because it is a point-to-point communication technology it does not provide the capability for lawful interception of the iMessage content via a wiretap order. Investigators were never able to access the content of the communications over Viber and iMessage.

Case 12: Heroin Overdose/CDS Distribution Investigation Impeded by Encrypted iPhone

In a recent heroin overdose case, the victim survived and agreed to cooperate with Montgomery County Police in the investigation against the heroin dealer. The victim provided consent to search their iPhone and provided the password. The victim advised there were texts to/from the heroin dealer regarding sale of the heroin responsible for the overdose. Even with the victim's cooperation and the fact that the victim provided the passcode, investigators were unable to complete a forensic extraction of the iPhone because the iPhone backups were encrypted on the device.

Case 13: Murder/Suicide Investigation Hampered by Encrypted iPhone

In a recent murder/suicide investigation, investigators discovered that the suspect sent texts before and after the homicide on their iPhone regarding the victim and the crime itself. Investigators were unable to circumvent the password or decrypt the data on the device, leading to a critical investigative gap regarding the content, date/time, and other information

regarding these text messages. These communications could have provided investigators critical information regarding communications that had occurred between the suspect and potential witnesses/persons of interest.

Case 14: Homicide Investigation and Prosecution Crippled by Encrypted Android Phone

In a recent homicide, police learned that the suspect specifically conducted research about committing the homicide on their cell phone. The phone is encrypted with both a numerical passcode and pattern lock. The Electronic Crimes Unit was unable to bypass this lock and decrypt the device. The data on this device is critical to proving the suspect's malicious intent, preparation, and other factors regarding culpability. The inability to recover or access this data has significantly impeded this investigation and subsequent prosecution.

Case 15: Cellular Service Provider Fails to Respond to Homicide Investigation

On August 17, 2015 a Houston Police Department (HPD) detective was assigned to investigate a double homicide and discovered the cell phone for one of the victims was missing. The detective completed a search warrant and a court order to track the cell phone and obtain historical records to determine where the phone traveled before, during, and after the victims were killed. This order was served on the cellular service provider on August 20th. The detective was told by the cellular provider to not expect a response for at least 48 hours, and the 48 hours did not include weekends or holidays. The cell phone company finally began providing the police with information late on Monday, August 24. They eventually provided the police with call history data that was incomplete. As a result, the detective has not been able to determine the victim's cell phone location and activity before their death.

Case 16: Cellular Provider Fails to Assist During School Terror Threat

On March 28, 2015 HPD detected a threat made online by a Twitter user that caused a local area high school to go on lockdown. The post threatened the school and responding police officers and included a photo of an assault rifle. Twitter stated this situation did not meet the definition of an immediate life threatening situation. A search warrant was obtained by HPD that demanded immediate release of information, but it took Twitter two weeks to respond with any information. Through the course of the investigation HPD learned the sender used a free Virtual Private Network (VPN) service to hide their location while posting the threat(s) on Twitter. The VPN service was used to mask the Internet Protocol (IP) address of the device posing the threat to make it hard to track the activity back to the suspect. As a part of the continuing investigation, HPD issued a court order to the VPN service on April 23, 2015 requesting assistance. On May 12, 2015 the CEO of the VPN company responded by saying that activity logs are purged every 48 hours (well before the two week delayed response from Twitter) and was not able to find any records matching the IP address. However, they were able to geolocate six VPN user accounts that were created the day of the threat near the threatened high school using a cell phone. In part because of the delayed response from Twitter, no suspect has ever been identified.

Case 17: Cellular Provider Fails to Comply, Hindering Search for Wanted Fugitive

On August 13, 2015, HPD Financial Crimes Division needed assistance in locating a fugitive suspect. A search on one of the suspect's phone numbers resulted in the discovery of an application that hid the fugitive's location. The application-based service which runs on a smart phone device and provides a secondary phone number not native to the phone and is invisible to the carrier of record. A search warrant was issued and served and the information obtained from the application company showed that the application was being used on an Apple device. The application company also provided two Identifiers for Advertising (IDFAs) given to the application company by Apple related to the device. A second search warrant to Apple was issued requesting the IDFA conversion details to be able to uncover additional device-specific information (e.g., type of device, cellular number attached to the device) or any other information to identify the suspect and critical information that could lead to their location. The police agency served the search warrant to Apple and received a response stating that no information was found. Apple's response with no data thwarted the government's effort to capture a wanted fugitive.

Case 18: Encryption and Incomplete Response Denies Justice to Murder Victim

On May 29, 2014 HPD responded to a homicide. During the course of the investigation detectives learned that the victim was using the Kik instant messaging application. Kik is based in Canada and will not respond to a lawful process issued in another country. HPD obtained four search warrants for other information from two service providers. One service provider responded but the other initially replied that they did not have additional information. A second warrant was issued requesting the same information and they replied with an incomplete set of data. In the continuing investigation the Homicide Division worked with the U.S. Department of Justice (USDOJ) to process a Mutual Lateral Assistance request (MLAT) through existing treaties between the U.S. and Canada. It took approximately 9 months for the process to work its way through the USDOJ to Canadian courts before Kik responded with data related to the case. Only one photo and no chat content was provided in the responsive records, providing no assistance to the investigation.

Case 19: Delayed Response Aids Suspect's Escape

On November 6, 2015 HPD responded to a double homicide in which a mother and her 23-month-old child had been shot to death. On the scene a suspect was quickly identified and it was determined that the suspect used a cell phone to call friends after committing the murder. Recognizing the urgent need to track the suspect before they were able to flee, the HPD quickly obtained a pocket warrant and a phone order for the phone. The service provider informed HPD that they generally take five days to track a phone, but police persistence enabled the phone to be tracked in four hours. By then, the suspect was an hour from the U.S./Mexico border and their phone went dead so they were unable to continue tracking. In part because of

the delayed response to the warrant, the suspect has not been apprehended and is thought to be at large in Mexico.

Case 20: Lawful Access Aids Investigation

On January 20, 2015 a text message ransom demand was send to a victim's mother using an application. The text message turned out to be a false ransom used to cover up a murder that had already occurred, but that was not initially known. At the time of this case the application was still being passed serial numbers of devices by the service provider. HPD was able to work with the application company to identify the suspect's phone and determine that the murder had already taken place. HPD was able to bring some closure to the family and the investigation thanks to the lawful access to information.

Case 20: Encrypted Messages Enable Narcotics Distribution

There is an ongoing high-level narcotics case in a major metropolitan area that is being hindered by the suspect's use of an encrypted texting application. There is no way to intercept the relevant communications in real time (the narcotics detectives have a court order for the phone and texts) and messages are immediately deleted from the server so the detectives can't subpoena them after the fact. Since the messages are encrypted, the provider cannot provide them in response to the warrant. All the detectives can tell is that a message was sent. The lawyers for the company say that is exactly the way they want it to work and that's the way it will keep working.

Case 21: Apple Protects Meth Dealer to Protect Image

In Brooklyn, New York a felony drug charge was brought against Jun Feng. Feng was charged with three counts of possessing and distributing methamphetamine. The government lawfully seized Feng's iPhone 5S, but because of its encryption the government needs help unlocking.

The manufacturer has refused to unlock the encrypted phone which likely has evidence of drug distribution crimes on it. The manufacturer's main argument is that assisting the government to unlock the phone would tarnish the company brand, despite being served with a lawful court-ordered warrant.

Case 22: Murdered Father's Killer on the Loose Because of Encrypted Mobile Devices

On June 8, 2015, a father of six was murdered and likely robbed in Evanston, Illinois. The police were able to recover two passcode-protected devices near the body, an iPhone 6 and a Samsung Galaxy S6 Edge running on Google Android. Prosecutors served the manufacturers with judicial warrants to unlock the phones, believing that relevant evidence might be stored on them which would be important to the investigation since there were no eye witnesses and there was no surveillance video available. Despite being served with a court order signed by a judge to unlock the phone, the companies who created the operating systems on the mobile

devices were unable to comply due to the use of full-disk encryption. The case remains unsolved and the killer or killers are at large.

Manhattan District Attorney Cases

The following is a list of recent cases from the Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety.[4] It includes cases in which evidence from devices that were able to be searched was helpful in either prosecuting or exonerating a defendant.

Case 23: Homicide, People v. Hayes, Indictment Number 4451/12
The victim was filming a video using his iPhone when he was shot and killed by the defendant. The video captured the shooting. Because the iPhone was not passcode-locked, the video was recovered and admitted into evidence at trial. The video corroborated eyewitness testimony. The defendant was convicted of murder and sentenced to 35 years to life.

Case 24: Rape and Robbery Conspiracy, People v. Sandel, Rivera, and Cruz, Indictment Number 3158/15
The defendants are charged with committing predatory sexual assault, conspiring to rape and rob several victims, and numerous related crimes. During some of the rapes, they used mace on the victims. Significant evidence against the defendants was recovered from phones belonging to two of the defendants. Internet browsing history relating to mace was found on a phone. Text messages between the defendants were also crucial. For example, Rivera sent a text message to Sandel stating in substance, "just bring that pepper spray & taser," and Rivera sent a text message to Sandel stating in substance, "Soon we will terrorize NYC again." On the highest charge alone, each defendant is facing up to 25 years to life.

Case 25: Child Pornography, People v. Hirji, Superior Court Information Number 3650/15
The defendant was arrested after he began speaking with a cab driver about his interest in having sex with children and after showing the driver a child pornography image. An iPhone and an Android tablet were recovered from the defendant. Investigators obtained a search for the devices, and a forensic analyst determined the passcode for

both. Upon searching the iPhone, investigators discovered a large number of child pornography images. The defendant was convicted of Promoting a Sexual Performance by a Child.

Case 26: Sex Trafficking, People v. Brown, Indictment Numbers 865/12, 3908/12, and 3338/13
The defendant directed a sex trafficking operation involving at least four women, using physical violence, threats of force, and psychological manipulation to coerce the women to engage in prostitution. Evidence recovered from electronic devices seized from the defendant's home proved crucial to his conviction at trial. In particular, the defendant's smartphones contained photographs showing him posing his victims for online prostitution advertisements, and showing that he had "branded" multiple women, with his nickname tattooed onto their bodies; text messages between him and several victims confirmed that he had engaged in acts of violence against the testifying witness and others. The defendant was convicted of multiple counts of sex trafficking and promoting prostitution and was sentenced to 10-20 years in prison.

[4] Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, November 2015.

Case 27: Sex Trafficking, People v. Rosado, Indictment Number 5591/14

The defendant ran a sex trafficking operation involving multiple women and underage girls. He advertised their prostitution services on a website called Backpage, and used physical force to keep the girls and women in prostitution. When the defendant was arrested, he was in a car with a pregnant 16-year-old. An unlocked Android smartphone was recovered from him. Pursuant to a search warrant, our office analyzed the contents of the phone. Significant evidence was recovered, including text messages between the defendant and male customers about prostitution, the defendant's web browser history, which showed his access of Backpage, and photographs of the prostitutes that the defendant had posted in Backpage ads. This evidence was admitted at the defendant's trial. The defendant was convicted of Sex Trafficking and Promoting Prostitution, and sentenced to a prison term of seven to fourteen years.

Case 28: Cybercrime and Identity Theft, People v. Jacas et al., Indictment Number 42/12, and People v. Brahms et al., Indictment Number 5151/11

This case involved the successful prosecution of a 29-member identity theft ring. An iPhone was recovered from a waiter who was arrested for stealing more than 20 customers' credit card numbers by surreptitiously swiping those credit cards through a card reader that stored the credit card number and other data. When the phone was searched pursuant to a warrant, law enforcement officials discovered text messages between the waiter and other members of the group regarding the ring's crimes. Based in large part on information obtained from the phone, investigators were able to obtain an eavesdropping warrant, and ultimately arrested 29 people, including employees of high-end restaurants who stole credit card numbers, shoppers who made purchases using counterfeit credit cards containing the stolen credit card numbers, and managers who oversaw the operation. The group compromised over 100 American Express credit card numbers and stole property worth over $1,000,000. All of the defendants pled guilty, and more than $1,000,000 in cash and merchandise were seized and forfeited.

Case 29: Unlawful Surveillance, People v. Lema, Indictment Number 4117/13

The defendant was arrested for unlawful surveillance after a police officer observed the defendant using his phone to film up women's skirts, which is known as "upskirting." The defendant consented to a search of his phone, but the passcode he provided did not work. Investigators obtained a search warrant and unlock order for the phone. The phone was sent to Apple, Apple extracted data from the phone, and the phone and data were returned to the prosecutor. Two upskirting videos were found on the phone, both filmed on the date of the defendant's arrest. Following the trial, at which both videos were entered into evidence, the defendant was convicted as charged, of two counts of unlawful surveillance. Had the defendant been using an iOS 8, these videos would not have been recovered.

Case 30: Homicide Exoneration: People v. Rosario, Indictment Number 1859/10

A detective obtained a search warrant and an unlock order for certain iPhones found at the scene of a homicide. He sent the phones to Apple, which assisted in extracting data from them. The phone data demonstrated inaccuracies in what investigators initially thought to be the timeline of the events, and that a particular suspect was not, in fact, involved in the murder. A phone number stored in one of the iPhones was eventually linked to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 1/2 years' imprisonment.

Appendix B: Press Coverage, Testimony, and Documentation on the Issue

This white paper does not endorse any particular news outlet or journalist, but provides these links for situational awareness purposes.

1. Written Testimony of the FBI Director James Comey before the Senate Judiciary Committee, December 9, 2015 FULL TEXT
2. Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, November 2015 FULL TEXT
3. Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the United States Senate Committee on the Judiciary, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," Washington, D.C. July 8, 2015 FULL TEXT
4. Apple and Other Tech Companies Tangle With U.S. Over Access to Data (9/7) FULL TEXT
5. Apple would not comply with warrant because of encryption (9/8) FULL TEXT
6. The Bangkok bombers reportedly never met in person—they planned the attack on WhatsApp (9/8) FULL TEXT
7. The Brittney Mills murder case has put Baton Rouge in the middle of the national cell phone encryption debate (8/30) FULL TEXT
8. (British) Police chiefs: We can't cope with cybercrime: Stunning admission in secret briefing shows toll of criminals exploiting the 'dark web' (8/29) FULL TEXT
9. When Phone Encryption Blocks Justice (Op-Ed – 8/11) FULL TEXT
10. DOJ calls for encryption balance that includes law enforcement needs (8/12) FULL TEXT
11. Prosecutors cite Evanston case in call to defeat encryption (8/11) FULL TEXT
12. British Teen Admits to Advising on Australian Terrorism Plot (7/23) FULL TEXT
13. FBI, Justice Dept. Take Encryption Concerns to Congress (7/8) FULL TEXT
14. FBI chief warns encryption emboldens would-be Islamic State attackers (7/8) FULL TEXT
15. Why phone encryption could stymie local law enforcement (7/8) FULL TEXT
16. Internet firms to be banned from offering unbreakable encryption under new [United Kingdom] laws (11/2) FULL TEXT
17. FBI opens facility to assist state and local law enforcement investigate digital and electronic crime, but faces challenges with encryption (11/5) FULL TEXT
18. SCRIPPS Investigation reveals encryption technology hampers law enforcement (11/5) FULL TEXT