HARRIS COUNTY
HCSO
SHERIFF'S OFFICE

SHERIFF RON HICKMAN

1200 Baker Street, Houston, Texas 77002 ★ (713) 755-6044 ★ www.sheriff.hctx.net

April 11, 2015

The Honorable Tim Murphy
Chairman
Subcommittee on Oversight and Investigation
Committee on Energy and Commerce
U.S. House of Representatives

Ref: Hearing Entitled "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"

Dear Congressman Murphy,

First, let me introduce myself to your committee and provide some basic background and qualifications. I am a forty-five year peace office and currently the Sheriff of the third largest Sheriff's Office in the Country. I currently serve as Chairman of the Local Executive board for the Greater Houston Regional Computer Forensic Labs and sit on the FBI's National Advisory Board providing local input for the network of seventeen regional computer forensic labs across the country. I have been supervising technical investigators and been involved in such cases for at least twenty years.

In general, the issue at hand is about how to gain access to data stored on electronic devices, ie a cell phone or other portable device with a unique operating system. The government's approach in the case of the phone belonging to the San Bernardino shooters seems to seize the opportunity of a high profile incident with a compelling public interest and a nexus to terrorism to compel technology companies to provide a tool or back door access to the device and its data. Such a tool would seem to bypass the device's immediate limitations to access or locks on the user interface, or front end of the operating system, and gain access to the phone's functionality. Encryption of the actual data layer may be another issue entirely.

Law enforcement has always followed a set of rules surrounding access to evidentiary data authorized under court order on a case by case basis, based solely on the justification provided to a qualified member of the judiciary. Should the justification rise to the level of the issuance of a search warrant in any case, that warrant is always limited to the circumstances specified. This tool would bypass that level of judicial scrutiny. Many believe that the 4th Amendment tenets should remain inviolate and in bypassing this requirement and requiring companies to provide such access would erode the delicate trust we try to maintain with the public. In researching the issue with my staff experienced in the matter, we provide the following:

1) Should US Technology companies be forced to install backdoors on their products to permit government access to encrypted data?
   a) In reference to requiring companies create a product is a very sensitive subject and I know of no place in the constitution which allows for the government to require a

company create a product. This would create a situation in which the company creating the product/back door could arguably be considered an agent of the State. At which point does the 'product' become the Intellectual Property of the State? Will the Government then require the company provide unlimited free updates and new versions? Based on previous records, how will the Government ensure the safety and privacy of the product as it will be disseminated to the various law enforcement agencies? Who will be the keeper of the Key?

2) Should Congress weigh in on this matter? Should Congress pass legislation to prohibit a government mandated backdoor?
   a) There are currently two States (New York and California) in the process of introducing laws which would ban the sale of phones with "full-disk encryption". This piecemeal approach would only serve to create confusion and conflict within the United States. This is one area where a Federal legislative preemptive approach would be better suited. The legislation would be well suited to prohibit States from requiring manufacturer's compromise their product offerings by weakening encryption.
   b) The Federal Government issues standards and requirements for motor vehicle safety, not the States. By allowing the States to address this issue in different manners would only serve to create a new genre of laws concerning the exportation of encrypted devices among States. By addressing this issue on the Federal level would serve to keep a consistency across States for all manufactures and serve to create a more secure and competitive environment. How would a State disallow a cell phone from say, Texas, to work in a State like California which would require the compromise? Is this something the carrier would be required to monitor and maintain and at what cost to the carrier?

3) Should Congress mandate that a backdoor be installed under certain, limited circumstances, such as a warrant requirement?
   a) This would presume the technology already exist in order to implement, post act, the backdoor on a device. To initiate the inclusion of a backdoor on a device would require the device ALREADY be configured to accept the backdoor. This would mean the device was already in a compromised state. Prior to the issue presented by the FBI, and after the exposure of intelligence agencies acquisition of cellular/digital phone data through the extended use of the FISA courts beyond their initial mandated roles, this issue was a moot point. The fact the court is ultra-secret and has relatively no oversight and no truly viable method to appeal a ruling has created a situation in the public of extreme distrust and 'conspiracy theories' are constantly voiced by the public. Local law enforcement, have taken a direct hit in the ability to obtain information and records due to those actions. While we in local law enforcement have always strived to be transparent and open as to the content and scope of our search warrants for data/access through the accepted use of search warrants, it would seem the DOJ has not and this has created a very real backlash within the realm of privacy. Again, the concept of forcing a company to create a 'back door' is not one path the Congress should tread. By doing so would foster distrust not just between the public and the Government but also between the private sector manufacturers and law enforcement. We must address the issue in a collaborative effort and not in an adversarial one.

4) How would the inclusion of a backdoor affect the competitiveness of U.S. technology abroad?
   a) By requiring the creation of a back door to software places American companies in a weaker position in the very competitive global market. This requirement would place our companies in a position of not being providing their customers a truly secure and mature product when overseas competitors in overseas markets are not burdened with this mandate. This would serve to create a situation where companies already struggling to differentiate themselves from the competition would find it difficult not to relocate out of the United States in order to stay competitive in the global economy. The current projected growth in overseas markets is substantially more progressive as global population densities change. Legislating the inclusion of a security compromise erodes the trust in corporate America as those in other countries will always be left wondering if American made products are just an extension of the American Government's intrusion into private communications.
   b) Another issue which must be discussed is what happens if another Nation State obtains the process and procedures put in place by the US Government. This would now provide those countries with the ability to obtain information from our communications. This does not include the bad actors, including Nation States, from obtaining the information thereby placing US interests in substantial risk.
   c) By forcing technology companies to provide backdoor access to devices and processes would only serve to weaken the systems in place to protect consumers from identity theft and other technology facilitated crimes. This includes the online market in which all data transmitted across the networks of the carriers is encrypted to protect the end user. To weaken this process only serves to provide a target for criminals and hackers alike. Many users have transitioned to using mobile devices for their banking and financial transactions and rely heavily on the high level of encryption

5) What would the implications of a Government-mandated backdoor mean for the U.S. technology in other countries? Would other countries be given the key to the backdoor as well?
   a) Given the current accelerating trend towards more and more secure private communications, technology created in the US would be substantially more vulnerable to outside hacking. If our devices and technology are not secure due to a designed in compromise, other countries and entities will not allow our devices on their networks to process financial transactions. Something as simple as checking your bank account with your phone could theoretically be denied due to a weakness in the platform. For many years, several banks forced the end users to update their computer's web browser because the encryption technology was not sufficient to provide adequate protection against compromise. What will happen when all U.S. Technology providers are required to build in a compromise to their system? Think of it this way, if you take a cell phone from the US with our technology, which includes a built in back door, to another country, it would be like painting a giant red X on it and advertising it as a device with a known weakness which has been built in by the manufacturer. With our devices in a constantly connected state, it is not difficult to envision bad actors spending large amounts of resources and money in order to identify those devices on the network in order to compromise the entire

system. This act of actively seeking those devices could lead to slower networks as they are flooded with traffic probing for their presence.

All of the above answers to the proposed questions are based around mobile device technology. What happens when the Government decides to address these issues in encryption technology in general? Does the Government provide for itself an exemption to the rule of law if one is passed? How does this type of approach directly affect the U.S. financial market as everything transmitted is done with a very high level of encryption to protect the data. Encryption is used in everyday communication both in the mobile telecommunications world and on the Internet. Something as simple as going to www.google.com ends up with encryption technology being employed to prevent others from seeing your web traffic.

From an article on Engadget.com written by Ms. Violet Blue (tinynibbles.com, @violetblue) is a freelance investigative reporter on hacking and cybercrime at Zero Day/ZDNet, CNET and CBS News

http://www.engadget.com/2015/11/19/lets-have-an-argument-about-encryption/

"…… even before the Paris attacks, Tim Cook had to patiently explain like a seasoned parent that "any backdoor is a backdoor for everyone. Opening a backdoor can have very dire consequences."

An excellent article from Tech Times

http://www.techtimes.com/articles/129680/20160202/myth-busters-harvard-edition-harvard-study-makes-compelling-argument-on-encryption-and-going-dark-government-fears.htm

"A new Harvard study stands by companies that use software encryption in products, explaining that authorities will have abundant amounts of data to feed their surveillance hunger.

The study shows that the ever-growing Internet of Things gives law enforcers access to a myriad of information pertaining to the user of the connected devices. The transformation of traditional households into Smart Homes gave birth to the Internet of Things, which comprises everything from vehicles and smart TVs to IP video cameras, all of which are Internet connected.

"Law enforcement or intelligence agencies may start to seek orders compelling Samsung, Google, Mattel, Nest or vendors of other networked devices to push an update or flip a digital switch to intercept the ambient communications of a target," the report says (PDF)."

Suffolk County DA Daniel Conley has a written testimony, which when researched online, does hold validation even though many in the media world would like to discredit his assertions. He brings to light some of the issues which Law Enforcement face when dealing with encryption on cellular devices.

http://motherboard.vice.com/read/the-latest-argument-against-apples-new-encryption-its-for-perverts

"But a Massachusetts prosecutor, who is scheduled to testify at a House hearing on encryption on Wednesday, is taking the arguments a step further into bizarre territory.

If encryption becomes widespread, according to Daniel Conley, the Suffolk County District Attorney in Massachusetts, perverts that take surreptitious pictures of women's intimate parts on public transportation—also known as "upskirting"—will never be prosecuted.

"If the offender's phone can't be searched pursuant to a warrant, then the evidence won't be recovered and this practice will become absolutely un-chargeable as a criminal offense," Conley, who is also a board member of the National District Attorneys Association, will tell the House Committee on Oversight and Government Reform, according to the written testimony he submitted ahead of the hearing.

Conley, however, doesn't mention that the pictures might be in the pervert's cloud storage (phones sometimes have cloud backups turned on by default), which would potentially put them at the reach of police forces. He also doesn't explain how often his district prosecutes these types of cases."

The author of the article obviously has never had to walk in the shoes of an investigator seeking information for a case. He presumes law enforcement would know which cloud storage service to request the information. He apparently has never asked for information from a cloud storage service. Many of the services are now encrypted so the data in the cloud is also not accessible even with a court order. The DA is accurate if the data is not obtainable then the charges may not be considered since there is insufficient evidence to support a charge. This not only happens in 'upskirting' scenarios but many categories of offenses as well. This is the type of misconceptions which are furthered by the media which only serve to make this issue more difficult to bring to a mutually satisfactory conclusion for all parties. Balancing privacy with security has always been difficult.

In relation to the above article with DA Conley we can also add to this list several cases here within the HCSO which have been directly affected by the use of Encryption. One of our investigators is working a case very similar to the above in which a deputy is called out to a scene where the suspect had been observed taking photographs of a young girl under the divider of a dressing room. The deputy arrives on scene and speaks with the suspect and looks at the suspects cell phone. The deputy sees images which would be considered Invasive Visual Recordings (a State Jail Felony) and files the appropriate charges. The deputy then drops the phone as evidence and after an extended period of time the High Tech Crime Unit is notified about the case. An HTCU investigator retrieves the phone only to find it is locked and running encryption so all the evidence the deputy saw on scene is no longer available for the court. It is an Apple IPhone 4S running IOS 9.

Other notable cases

We have currently have a laptop in relation to a possible suicide/homicide in which the laptop was submitted as evidence. The laptop is a Macbook Pro 15 inch (late 2012) and when we attempted to image the drive using the newest and latest tools designed specifically for Apple products it was noted the laptop is running the newest version of Apples FileVault2. According to the FBI it will take approximately 34 years to brute force the laptop's encryption key using today's supercomputers.

Another case of note is U.S. vs Todd Ewanko. This is the airline pilot whom we arrested in 2010 for the possession of Child Pornography via file sharing networks. When the search warrant was executed we were extremely fortunate the suspect was awake and using his computer at the time. This means he had 'mounted' the drives in his computer – a total of 7 hard drives in one machine – and had opened his encryption program he was using. He finally provided the encryption keys for the hard drives and we discovered more than 26 million images of child sexual assault on his computers. If he had simply turned the computer off prior to answering the door, we would not have any of the evidence.

We also worked a case with the Houston Metro ICAC in which the suspect had only one image of child sexual assault on his main hard drive in his computer and it was only a thumbnail. The suspect refused to provide the password and it was only after the forensics examiner noted a document with a password in it were we able to access the external hard drive which was running encryption and was able to identify the person was sexually assaulting a child inside the residence and taking photos of the assaults. (Pasadena ISD PD Case)

We currently have a homicide case (15-133875) in which the phone is of the suspect who is an unknown but the phone is running IOS 9 or higher and is locked so no access can be made at this time. There are no other viable leads in this case other than data which may be on the phone.

I spoke with the Greater Houston Regional Computer Forensics Lab Quality Assurance Manager on 4-13-2016 and learned 20 percent of the devices presented to the Lab (this includes the devices submitted and those identified at the door as not viable and retained by the lab) are not accessible due to encryption running on the device. Just yesterday (4/12/2016) two devices were declined at the intake process on a very significant case out of Austin due to them being locked and being IOS devices.

The High Tech Crime Unit has processed 247 devices since 08-31-2015 from our own investigators and also outside agencies with approximately 17 devices considered as significant value to the investigation running either encryption or locked beyond our capability to access the underlying data. Significant value means the device is the only viable piece of evidence relative to the case. There were substantially more devices which were locked but ancillary to the investigation and not the main focal point.

During the time period of 2015-2016 (which I could locate in FileOnQ as "phones" in our reporting system since due to coding mismatches I am sure not all phones are listed correctly so

this is a conservative number) the HCSO as a whole took in 1457 phones in reference to cases under some form of investigation. Of the **1457** phones, the HTCU has processed **125** devices presented to us from HCSO investigators.

It should be noted the number of cases where we expect to see phones locked beyond our current capability to unlock them will substantially increase. This is due in part, our unit at the HCSO is new and the training for processing phones was recently completed. Also of concern is it was with IOS 8 where encryption began to be pushed out "enabled" by default and Apple placed most of the user data under the encryption of the passcode. With IOS 9 a new longer pin code was allowed along with a passcode if desired. This created a more robust security feature and complicated the attempts to brute force a pin code. With IOS 9 Apple initiated the 10 and your done rule where the phone would wipe or brick itself with 10 incorrect pass attempts. The older IPhones were easier to obtain access with the right tools and the right training. As of this year, that is no longer possible.

The chart below is for your reference to the cases where the phone is of significant value to the case.

Device Make	Device Model	Is Phone Unlocked	Password If Provided	Type Of Investigation
ZTE	Z432	YES	N/A	ICAC
APPLE	6 S PLUS	YES	NONE PROVIDED/12399	Death Investigation
APPLE	I-PHONE(A1549)	NO	N/A	Death Investigation
APPLE	I-PHONE 6	NO	N/A	Auto Theft
SAMSUNG	SM-G386T	NO	N/A	Auto Theft
APPLE	A1549	YES	LOCKED	Gang
APPLE	I-PHONE 4S A1387	YES	N/A	Death Investigation
APPLE	I-PHONE 4 A1387	NO	N/A	Death Investigation
APPLE	I-PHONE A1533	NO	N/A	Sexual Assault
APPLE	6 S PLUS	YES	NONE PROVIDED/12399	Death Investigation
LG	LGMS769	NO	N/A	Death Investigation
APPLE	I-PHONE 5	NO	N/A	Death Investigation

APPLE	I-PHONE 6 A1633	NO	N/A	Robbery
APPLE	I-PHONE 5	NO	N/A	Death Investigation
SAMSUNG	SM-G920T	NO	NO	Robbery
APPLE	I-PAD 32GB	NO	NO	Robbery
RCA	RCT 6773W2	NO	NO	ICAC

In conclusion, we might point out that encryption and restricted access is an issue that will continue to confront us and what we must consider is whether the government should, or to what degree, they will play a role in preparing us for that future need for access to data, as well as our ability protect it at the same time.

Sincerely,

[redacted]

Ron Hickman, Sheriff
Harris County
FBI NA #256