DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

1/27/20 RESPONSES FROM NY D.A. CYRUS R. VANCE, JR. TO THE QUESTIONS FOR THE RECORD RE: 12/10/19 SENATE JUDICIARY HEARING ON ENCRYPTION

Questions from Chairman Graham

Question 1:

Is getting content more important than getting metadata? Why?

Answer 1:

While metadata and content are both critical to understanding digital evidence, content is usually much more valuable from an evidentiary point of view.

Metadata, or data that describes other data, provides certain information about the content: file sizes, file types, dates and times, file names, and geolocation. For example, a digital photo's metadata typically includes the date and time the photo was taken, its filename, camera settings, and geolocation. The photo's image would be the content.

In a communication between two parties, the metadata provides information such as the time and duration of the conversation, while the content is the actual substance of the message. While the metadata is important, investigators need to know the content of the conversation to have insight into the parties' intent, collaboration, modus operandi, planning, execution, etc.

Metadata and content are both pieces of the puzzle when investigators analyze stored electronic data, and one cannot be substituted for the other. While useful, the metadata provides less substantive value into the most relevant questions for investigators, accused, and judges. Content is the key to proving an accused's guilt beyond a reasonable doubt, or ultimately exonerating individuals not responsible for criminal activity.

Question 2:

How many phones do you lawfully seize each year and how many of those phones remain locked because of encryption?

Answer 2:

In late September 2014, Apple and Google announced that they would encrypt their operating systems by default. The following chart reflects the number of mobile devices (smart phone, cell phone, or tablet) that my Office's forensic laboratory has received – either through lawful seizure or consent - since October 1, 2014.

Operating System

Year	Android	iOS	Other	All Devices
2014 (10/1-12/31)	122	99	105	326
2015	512	528	335	1375
2016	627	703	342	1672
2017	774	787	240	1801
2018	686	879	115	1680
2019	660	829	87	1580
Total	3381	3825	1224	8434

Of the 326 devices received in 2014, 79 were locked on arrival and we are still locked out of 61 of those devices.[1]

Of the 1,375 devices received in 2015, 605 were locked on arrival and we are still locked out of 371 of those devices.

Of the 1,672 devices received in 2016, 821 were locked on arrival and we are still locked out of 498 of those devices.

Of the 1,801 devices received in 2017, 878 were locked on arrival and we are still locked out of 490 of those devices.

[1] When we refer to devices that remain "locked," we are describing mobile devices that were locked on arrival and we were unable to circumvent the encryption during the pendency of the case. We may have been unable to access the device due to a lack of technology, an unwillingness to use cost-prohibitive technology, and/or the case resolved either through disposition or dismissal prior to our accessing the device.

Of the 1,680 devices received in 2018, 1047 were locked on arrival and we are still locked out of 666 of those devices.

Of the 1,580 devices received in 2019, 1035 were locked on arrival and we are still locked out of 405 of those devices.

	Locked on Arrival			**Totals of Devices Unlocked and Locked Out**		
Year	**Android**	**iOS**	**Other**	**All**	**Unlocked**	**Locked Out**
2014 (10/1 – 12/31)	19 (15.57%)	59 (59.60%)	1 (0.95%)	79 (24.23%)	18 (22.78%)	61 (77.22%)
2015	190 (37.11%)	383 (72.54%)	32 (9.55%)	605 (44.0%)	234 (38.68%)	371 (61.32%)
2016	257 (40.99%)	533 (75.82%)	31 (9.06%)	821 (49.10%)	323 (39.39%)	498 (60.61%)
2017	308 (39.79%)	553 (70.27%)	17 (7.08%)	878 (48.75%)	388 (44.19%)	490 (55.81%)
2018	310 (45.19%)	726 (82.59%)	11 (9.57%)	1047 (62.32%)	381 (36.36%)	666 (63.64%)
2019	331 (50.15%)	691 (83.35%)	10 (11.49%)	1035 (65.51%)	630 (60.87%)	405 (39.13%)

Question 3:

How much does cracking encryption cost the Manhattan DA's office on an annual basis?

Answer 3:

From October 2014 through December 31, 2019, my Office spent approximately $1.5 million dollars to access lawfully the data contained on encrypted devices. We spent approximately $1.1 million dollars on software and hardware used to circumvent encryption and extract data from mobile devices, and another $460,000 to train our staff.

Questions from Senator Grassley:

Question 1:

You testified about a number of hurdles that encryption creates in prosecutions and investigations. Short of a legal obligation to permit access to encrypted information, in what ways could industry be a better partner with law enforcement?

Answer 1:

There are a variety of ways in which industry can be a better partner with law enforcement. One relatively straightforward way to improve our partnership is for technology companies to be more transparent about what data that they possess and more timely in their responses to law enforcement requests. It is the experience of most state and local prosecutors that the industry simply takes too long to respond. Despite many hard-working individuals throughout the compliance teams of these multi-billion dollar companies, it is clear that the companies have not sufficiently resourced these teams. Perhaps this is because compliance is a non-revenue generating activity.

Once our requests are reviewed, they are often rejected for their purported failure to identify properly the requested data, or because the companies no longer possess the data requested. This issue could be alleviated if technology companies were transparent with respect to what data they collect, how long they retain it, and what they do with the data that they have collected, and accurately detail what data will be produced, and how long it will take to produce it, based on escalating legal process (i.e. subpoena, 2703(d) order, search warrant, eavesdropping warrant). Technology companies should also provide a definition of terminology used to identify the data they possess and should be required to notify law enforcement when they inevitably make changes to said terminology. Such information, coupled with a notice whenever a change occurs, would eliminate the wasteful guessing game that law enforcement is currently forced to engage in.

Question 2:

We talk about how encryption and "going dark" affects the ability of law enforcement to obtain evidence to prosecute criminals. Can this problem also impact law enforcement's ability to exclude individuals suspected of criminal wrongdoings or otherwise exonerate innocent people?

Answer 2:

The value of digital evidence is not limited to proving a defendant's guilt. In some instances, evidence recovered from devices mitigates the culpability of an accused, or exonerates a defendant entirely.

As we detailed in our 2018 Report on Smartphone Encryption and Public Safety, an internal survey of cases in our Office revealed seventeen cases in which we reduced or dismissed charges because of evidence recovered from a smartphone.

Below are several examples:

- In one such case, two defendants were identified as part of a gang assault in which a large group of people attacked three men and two women. Two defendants who were present at the scene were identified as participants by an eyewitness. Based on evidence extracted from one of the defendant's phones, it was determined that the defendants were not present for the assault at all, and they were exonerated prior to trial.

- In a similar case, an individual was identified as being one of multiple participants in an attack, based on an independent eyewitness. The accused claimed to have been chatting with friends on a social media application from another friend's phone at the time. Based on data from the social media app as well as cell site data for the phone, the defendant was shown to have been blocks away from the scene and not involved in the crime.

- In another case, a woman identified an individual as a person who had menaced her with a gun. The accused stated that he could not have committed the crime, because he had been in police custody at the time in connection with an unrelated matter. However, the accused could not corroborate his alibi. Through cell phone data and messages from the accused's social media applications, recovered during the execution of a search warrant on his phone, investigators were able to locate the precinct where he had been detained, and the date and time of his detention, and were able to determine that he could not have committed the gun-related crime.

- In a firearms investigation, evidence recovered from a cellphone revealed that the phone's user was not, as originally believed, the person seen by police throwing a bag containing a loaded gun. The evidence recovered included: 1) photographs of the defendant from the date and time in question wearing a

different outfit than the individual who was observed by the police, and 2) cell site data showing that the defendant was not in the area when the crime was committed.

- During an incident on a Manhattan street, a victim was slashed in the throat, causing a severe carotid artery wound. A suspect was charged with Attempted Murder and Assault. The defendant's phone was encrypted. After obtaining a warrant and after months of employing a workaround, the phone was unlocked, and we found video evidence which established that the defendant in fact did not commit the slashing.

We have repeatedly stressed that access to smartphone data is a criminal justice problem, not just a law enforcement concern. We are not alone in voicing these concerns. A November 22, 2019 New York Times article highlighted the problem of inaccessibility for criminal defense attorneys and their clients.

> Jeffrey D. Stein, a public defender in Washington, D.C., recently wrote an opinion piece for The Washington Post on the subject of exculpatory evidence remaining trapped online. "Innocent people will continue to be vulnerable to conviction, not because evidence of their innocence doesn't exist, but because the law doesn't permit them to reach it," he argued.[2]
>
> "Funding is always the obstacle, [but] this should be mainstream across the country," said Tina Luongo, the lawyer who founded the Legal Aid Society of New York City's forensic lab. "It's the clients' constitutional right. It exonerates our clients and helps us bring them justice."[3]

[2] Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone. Public defenders lack access to gadgets and software that could keep their clients out of jail.* New York Times, November 22, 2019, available at. https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html

[3] Id.

From Senator Klobuchar:

In your testimony, you referred to a paper by the Carnegie Endowment for International Peace's Encryption Working Group, which describes the potential for a "middle ground" in smartphone encryption where the decryption key is on the device and access requires physical control of the device. The paper also describes eight principles that should guide any proposal in this area.

Question 1:

Do you support the "middle ground" as described in the Carnegie report?

Answer 1:

I do support the middle ground approach described in the Carnegie Report. Since 2015, when my Office published our first Report on Smartphone Encryption and Public Safety, I have taken the position that Congress should begin with data at rest.

I recommended this approach for several reasons. First, state and local law enforcement offices like mine handle the vast majority of criminal cases in the nation, and the digital evidence in our cases is more frequently data at rest. As such, it would make sense to begin with what would have the biggest positive impact. Second, the public's concerns about governmental overreach apply far less to searches of an accused's physical device than the interception of real-time communications. Third, there are more legal, technological, and jurisdictional challenges associated with data in motion than data at rest. Given the urgency of finding a path forward, I recommend that legislators begin with data at rest.

Moreover, the law treats these categories of data differently, and generally affords greater protection to data in motion. For example, the Stored Communications Act (18 USC §§2701-2713) authorizes the government to obtain stored electronic communications (data at rest) with a search warrant. By contrast, the Wiretap Act (18 USC §§2510-2523) requires the government to obtain a wiretap order – which carries additional proof requirements, and may only issue in certain types of investigations – to intercept electronic communications (data in motion). My Office's position follows that framework, and focuses on the type of data that – as lawmakers have recognized – should be available to law enforcement with a search warrant based on probable cause.

Question 2:

In your view, do the principles described in the Carnegie report strike the right balance between the needs of law enforcement and personal privacy rights?

Answer 2:

Yes.