Written by **C. Mitchell Shaw** on January 1, 2016

# Manhattan DA Fails to Make the Case Against Encryption

In late 2014 and early 2015, Apple and Google made better encryption technology an integral part of the iOS and Android operating systems, making the smart phones more private and more secure. The encryption used by the companies allows users to control their own data, making it inaccessible to anyone who does not have the password. This means that users can protect the personal information stored on their phones from criminals and overreaching government agents. The surveillance hawks in government have responded with calls for weakening the type of encryption used on mobile devices.

Prominent voices within the intelligence and law enforcement communities say full-disk mobile encryption places users "beyond the law," because — even with a warrant — the only way they can access the data is for the user to provide the password. Last month Manhattan District Attorney Cyrus Vance, Jr. released a report claiming that such encrypted devices pose "a threat to law enforcement efforts" and are "a boon to dangerous criminals." His report calls for new laws to compel companies to build backdoors into the encryption used on mobile devices so that the companies can search the devices when a warrant is issued.

Vance — whose father was President Carter's secretary of state as well as serving under Presidents Johnson and Kennedy as deputy secretary of defense and secretary of the Army — has a long family history of serving the interests of big government. As Manhattan's top prosecutor, he has followed in the family tradition.

In his 42-page report, Vance asserts that without the ability to decrypt and search mobile devices, law enforcement's hands are tied "because much important data may be found only on smartphones." His claim is the standard fare offered up by surveillance hawks. In this age of ubiquitous surveillance, too much is never enough for those whose careers are built on spying on others. Even with the ability to read e-mails and texts, listen to phone calls, harvest browsing histories, scan license plates, and otherwise conduct mass surveillance on the population at large, they claim that without outlawing the ability of citizens to use strong encryption on their mobile devices, law enforcement can't protect those same citizens from "criminals and terrorists."

Of course, they make the same claim about all of the other surveillance techniques they use, too — even those which violate the Constitution and likely violate state and federal laws. You see, they need it *all* or they can't do their jobs. While Vance claims that "much important data may be found only on smartphones," it is a fact that police were able to investigate crimes and district attorneys were able to get convictions before the advent of the smart phone. Why can't they do so now? As this writer noted in a previous article:

> The problem is that law enforcement at almost every level has become addicted to the easiest path.

> Many in law enforcement prefer to conduct investigations using surveillance techniques instead of using more time-consuming methods. They don't seem concerned that their surveillance does more to injure the privacy and liberty of the law-abiding citizens than it does to build solid cases against criminals and terrorists. The evidence for that is that in many cases, prosecutors have dropped charges or agreed to forgo having evidence admitted if it meant revealing the (likely illegal) use of blanket surveillance.

So, the truth is that police and prosecutors *could* do their jobs without new laws banning the current use of full-disk encryption on mobile devices. Many of them just don't have the practiced experience of doing so because they have for so long simply depended on digital surveillance instead of actual investigation. Vance's report comes dangerously close to admitting this by saying, "It is the rare case in which information from a smartphone is not useful." The natural implication of that is that it is also a "rare case" where police and prosecutors do not treat every smart phone as if it were a trove of information just waiting to be sifted through.

Granted, it may be easier to conduct investigations and successfully prosecute crimes by gathering data from every (or nearly every) smart phone of every (or nearly every) suspect. It is therefore harder to do so without harvesting data from all those phones. But police and prosecutors have a responsibility to do their jobs without damaging the privacy of every (or nearly every) citizen.

After spending six pages claiming that "smartphone encryption has caused real — not hypothetical — roadblocks to our ability to solve and prosecute crimes," Vance takes up the challenge that has been issued time and again by privacy advocates: Prove it by credibly citing cases where, all other things being equal, encrypted devices have kept law enforcement from doing its job. He spends more than three pages trying to prove his case. And he fails.

The report claims:

> Between September 17, 2014 and October 1, 2015, the Manhattan District Attorney's Office was unable to execute approximately 111 search warrants for smartphones because those devices were running iOS 8. The cases to which those devices related include homicide, attempted murder, sexual abuse of a child, sex trafficking, assault, and robbery.

What the report does *not* say is how many of those cases were successfully prosecuted even without extracting data from the devices in question. Also conspicuously absent is any information about the cases. As is so often true in these claims, the claim itself is treated as proof, without any real proof being offered.

The report then lists eight cases "in which evidence from devices that were able to be searched was helpful in either prosecuting or exonerating a defendant." While making the claim that "There are many other cases — almost too many to count  that could have been selected," Vance holds these eight up as his evidence. It is reasonable to conclude that, as a prosecutor, he would not likely have listed the weakest examples he had to offer. If these cases are the best evidence he could present, he has little to offer in the way of a compelling argument.

Of the eight cases Vance chose as his examples, two involve homicide, two child pornography, two sex trafficking, one rape and robbery, one unlawful surveillance (peeping Tom), and one identity theft. In not one of the cases was a phone encrypted with the newest encryption. In all the cases, other evidence was available and assisted the police and the prosecutors in the performance of their duties.

In one of the homicide cases, a video on the phone in question was used only to corroborate eyewitness

testimony. In other words, in the absence of that video, the police and prosecutors would have had all the information they needed to conduct their investigation and prosecute the case.

In the other homicide case, multiple iPhones were found at the scene of the crime and sent to Apple for the data to be extracted. According to the report, "phone data demonstrated inaccuracies in what investigators initially thought to be the timeline of the events" which eventually led to the suspect not being charged. There are at least two points that need to be made here. First, this goes to the earlier point that in an era in which police and prosecutors lean heavily on digital surveillance, they tend to rely on it rather than on good investigative techniques. Smart phone data should not be required to correct the errors of investigators. Second, the mere fact that the data was discovered and the suspect exonerated, is not evidence that he would have been convicted in the absence of the phone data. That is a supposition that is not supported by any other information offered in the report.

In both the child pornography case and the peeping Tom case, there were witnesses to the crimes. In all the cases there was other evidence. Several of the devices were searched only after police had arrested the suspects, showing that even before searching the devices, investigators felt they had enough evidence to make the arrests. While the data collected from the phones may have made the work of police and prosecutors easier, it is more than a stretch to say their jobs would have been impossible without it.

As this writer noted in a previous article, "The truth is that criminals make mistakes just like everyone else, and skilled investigators are trained to find and use those mistakes in order to solve cases." The eight best cases Vance could produce to substantiate his claim that encrypted devices pose "a threat to law enforcement efforts" and are "a boon to dangerous criminals," fail to prove that. Instead they prove that criminals make mistakes and investigators — even those addicted to digital surveillance — can do their jobs. And they can do so with or without endangering the privacy of everyone else.

The danger to privacy exists because of the ubiquitous surveillance conducted by government at all levels. The very encryption Vance and his fellow hawks condemn is merely the free-market response to that surveillance. Apple, Google, and other companies would not spend the time, talent, and treasure to develop such technology products if the market did not demand them. The market would not likely demand them were it not for the intrusive, overreaching surveillance conducted by law enforcement at all levels.

Vance's report attempts to distinguish between the type of surveillance conducted by federal agencies and that conducted by state and local departments, but whatever distinctions exist are irrelevant. Police departments all over the country regularly use cell-site simulators to vacuum up data from all mobile devices within range of the simulators. Vance considers that type of surveillance acceptable because suspects and other citizens are supposedly protected by the Fourth Amendment. His report says:

> The Fourth Amendment dictates that search warrants may be issued only when a judge finds probable cause to believe that a crime has been committed and that evidence or proceeds of the crime might be found on the device to be searched. The warrant requirement has been described by the Supreme Court as "the bulwark of Fourth Amendment protection," and there is no reason to believe that it cannot continue to serve in that role, whether the object that is to be searched is an iPhone or a home.

But the fact is that when police use cell-site simulators, they often do so either without ever obtaining warrants or by misleading judges into issuing the warrants. Furthermore, considering that judges issue

warrants for intrusive searches based on no more probable cause than a suspect drinking tea and shopping at a gardening store, it is clear that warrants aren't what they used to be. Vance will have to understand if citizens feel they need a little more protection.

The report concludes by echoing the oft-repeated mantra that if new laws aren't passed to force companies to build backdoors into the encryption they offer, mayhem will ensue:

> Technology benefits us in ways too many to count and in amounts impossibly large to calculate. But it can also be used to harm us, and unless we regulate it intelligently and carefully, we may suffer great harm. Smartphones are technological bank vaults, but unlike bank vaults, which, no matter how strong, are accessible to search warrants, smartphones are becoming beyond the reach of law enforcement. The result will be crimes that go unsolved, harms that go unanswered, and victims who are left beyond the protection of the law.

The reality is that by regulating technology and weakening encryption, Vance and his fellow hawks will make more people more vulnerable to crime. Criminals and terrorists are using encryption and there is nothing that can be done to stop that from happening. Passing laws has not kept them from using guns and explosives and it won't keep them from using encrypted devices. Law-abiding citizens need the ability to use that same technology to protect themselves from both criminals and those in government agencies who would violate their rights. If investigators and prosecutors can't do their jobs because citizens use encrypted devices, then — rather than new laws — perhaps what is needed is new investigators and prosecutors.