Written by **C. Mitchell Shaw** on December 1, 2017

Manhattan DA Demands Encryption Backdoors

Manhattan District Attorney Cyrus Vance, Jr. is again attacking the encryption that protects data stored on millions of smartphones nationwide. Vance — a consummate surveillance hawk — claims that "traditional investigative techniques" no longer work in a world of "warrant-proof smartphones that have been designed to keep law enforcement out." His solution? Legislation that would grant police a backdoor into mobile devices.

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 a report issued by his office last week, Vance said tech companies such as Apple (maker of the iOS platform) and Google (maker of the Android platform) must be forced to alter the encryption standards used to protect the data stored on devices running those operating systems. This is not Vance's first run at this. He issued similar reports in 2015 and 2016. This new report is little more than a regurgitation of those previous screeds.

Vance's 2015 report, followed by the San Bernardino shooting that resulted in 14 deaths, led to the introduction of a bipartisan anti-encryption bill sponsored by Senators Richard Burr (R-N.C.) and Dianne Feinstein (D-Calif.) that would have forced tech companies to build in an encryption backdoor to be used only by law enforcement and only with a valid warrant — as if such a thing were even possible. A backdoor is merely a weakness in the encryption standard that *anyone* could exploit — with or without a warrant. As the *Wall Street Journal* quoted Donna Lieberman, head of the New York Civil Liberties Union, as saying, "There's no such thing as a backdoor that is just for law enforcement."

Besides that, warrants aren't what they used to be, either. Consider that a federal judge issued a warrant for a SWAT team to raid the home of a family in Kansas in 2012 — a warrant that was based on no more probable cause than members of the family drinking tea and shopping at a gardening store. Given the nature of the surveillance hawks to overstep even the wide and self-appointed "boundaries" they are supposed to abide by, their promises of behaving themselves with backdoors into encryption are hard to take at face value. Given warrants such as that, it is no wonder that millions of Americans choose to encrypt their data.

Even in the wake of the San Bernardino terrorist attack — and with Vance, Burr, Feinstein, and others (including then-FBI Director James Comey) waging a public-relations war against encryption — the anti-encryption bill of 2015 fizzled and died. But even as it was doing so, the surveillance hawks were fighting a losing battle on another front: The FBI was trying to get the courts to force Apple to hack into the phone of Syed Farook, one of the San Bernardino terrorists. When the House Judiciary Committee weighed in on the issue in March 2016, Comey had Vance join him in testifying before the committee. Birds of a feather (especially surveillance hawks) really do appear to flock together.

And while Comey was demanding out of one side of his mouth that Apple weaken its encryption and promising out of the other side that the tool he demanded would only be — *could* only be — used on that one phone, Vance was much more forthcoming. He told the committee that such a tool could have far-reaching implications for law-enforcement agencies across the country. In a prepared statement he read in his testimony, he said:

> While the San Bernardino case is a federal case, it is important to recognize that 95 percent of all criminal prosecutions in this country are handled at the state and local level, and that Apple's switch to default device encryption in the fall of 2014 severely harms many of these prosecutions.
>
> And that is why I am here today as a representative of the thousands of local and state prosecutors around the country: Smartphone encryption has real-life consequences for public safety, for crime victims and their families, and for your constituents and mine. In the absence of a uniform policy, our nation will effectively delegate the crafting of national security and law-enforcement policy to boardrooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google, and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.

In case that wasn't clear enough, Vance added, "Law-enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest."

But the opposition point is this: You cannot trust the surveillance hawks to limit themselves. Give them a kilobyte and they want the whole hard drive.

In his newest iteration of his report decrying the evils of encryption, Vance — who in 2016 said his office was in possession of 175 phones he wanted to unlock — says that in the first 10 months of this year alone, his office has recovered 700 encrypted devices he would like to have backdoors into. In other words, his office is escalating its attack on encryption.

A fine point the surveillance hawks consistently ignore is this: American citizens did not start the Crypto Wars — Big Brother did. The nearly ubiquitous encryption used by millions is a reaction to overreaching government and law-enforcement agencies headed by surveillance hawks. As this writer observed in December 2015, when Burr called for encryption backdoors:

> For all the ostensible reasons that the intelligence and law-enforcement communities give for wanting to limit the ability of ordinary citizens to encrypt their data and communications, the real reason is that those in power love power and want a monopoly on it. Government officials — who use encrypted systems for both data storage and communications — don't want private citizens to use that same technology. These are the same individuals who go about their daily lives surrounded by armed police officers, military personnel, and private security guards while decrying the evils of an armed society. This double standard is more than mere hypocrisy; it is tyranny.

As in his 2015 and 2016 reports, Vance failed to make a case for backdoors. This new report follows that same trend. In previous reports, Vance offered claims instead of evidence (one assumes he does not use that tactic in prosecuting cases before the bar of justice). For instance, the 2015 report claimed:

> 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.

As this writer wrote at the time:

> 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.

Of course, even if Vance could list scores of cases where accessing encrypted data helped his office successfully prosecute cases, it would still not justify sacrificing the privacy of millions of Americans.

In his new report — which is little more than an attack on privacy — Vance appears to be taking a different tack; he attempts to appeal to democracy. Claiming that the expense of "lawful hacking" to access the data on encrypted devices is prohibitive to all but the most well-funded offices, he writes:

> As technology companies continue to roll out new devices, workarounds become less available and more expensive, creating a landscape in which solving crime depends largely on a law enforcement agency's ability to spend money on private-sector solutions. This "privatization" of crime fighting is exactly the "arms race" predicted in the 2015 Report, which will result in greater and greater expenditures on the part of federal, state, and local governments. More problematic, it will result in unequal access to justice for crime victims across the country.

His point — aimed squarely at the emotional idea of "fairness" — completely misses the real point: Law-enforcement agencies have the responsibility to investigate crimes without sacrificing the liberties of the people they are supposed to protect and serve. Weakening encryption does not fit that description.

New anti-encryption legislation is likely on the near horizon. And President Trump — who as a candidate attacked Apple over its decision to resist weakening encryption — has filled some key Cabinet positions with surveillance hawks. The Crypto Wars could be getting ready to heat up.

Photo of Cy Vance, Jr.: Cyvanceforda