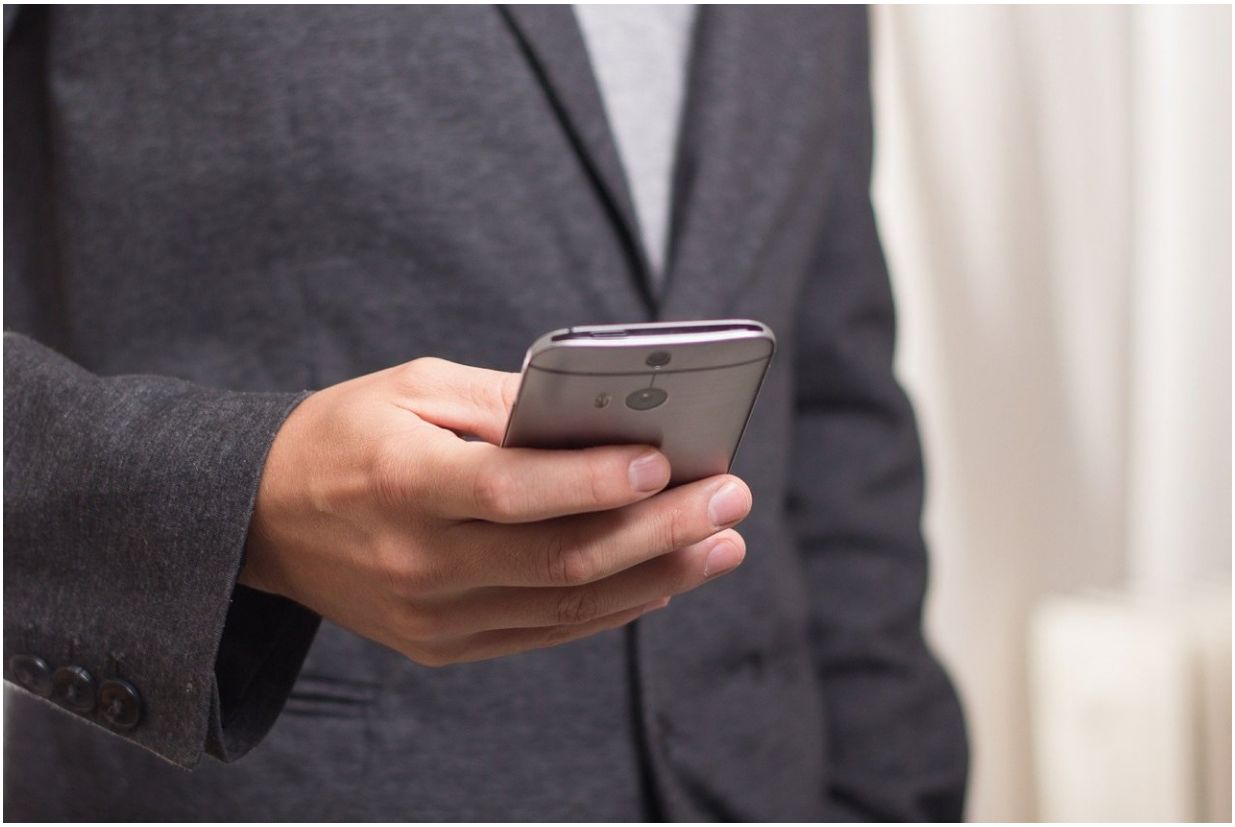
The epicenter of law enforcement's battle to unlock encrypted smartphones

February 12 2020, by Kevin Johnson, Usa Today



Credit: CC0 Public Domain

Inside a steel-encased vault in lower Manhattan, investigators are bombarding an Apple iPhone 7 with a jumble of numerical codes generated by nearby computers.

The grinding exercise has continued for the past 21 months with a singular aim: Crack the phone's passcode so police can extract potential evidence in an aging attempted murder investigation.

Despite the formidable resources of a $10 million cyber lab operated by the Manhattan District Attorney's Office—including costly assistance provided by private sleuths—so far the phone has won.

Last month, Attorney General William Barr revived the titanic struggle between law enforcement and Big Tech when he disclosed that the FBI couldn't unlock two iPhones used by a Saudi officer who opened fire at a Navy base in Florida in December.

Yet the breadth of the ground war waged against encrypted phones, tablets and other devices seized in criminal inquiries is perhaps best appreciated within the secure doors of this Manhattan laboratory.

More than 8,000 devices have poured into the facility since 2014. Each year, more of them are locked, rising from 24% in 2014 to 64% last year. For Apple devices, it's gone from 60% to 82%.

Nearly 2,500 of the locked devices remain inaccessible to investigators, hindering investigations into child exploitation, financial crimes, theft, violence and other crimes.

The numbers illustrate a frustration shared by law enforcement agencies across the country.

"I don't think there is an awareness of the scope of the problem," Manhattan District Attorney Cyrus Vance said.

Duffie Stone, president of the National District Attorneys Association, described the challenge as a "technological tidal wave" overwhelming

agencies across the country, particularly smaller ones without Manhattan's considerable resources.

However, it's been difficult to measure how much of a problem locked devices are for law enforcement. There is no national data repository tracking how often investigators are blocked by phones "going dark," as they say.

In 2018, the FBI estimated federal authorities had recovered nearly 8,000 locked phones for analysis. But the bureau acknowledged that figure was overstated. The FBI has not publicly updated the data since, leaving Vance as law enforcement's most vocal authority in the struggle between law enforcement and privacy interests.

Tech giant Apple is law enforcement's favorite target because of its commercial popularity and its efforts to bolster user privacy. In the past six years, law enforcement officials maintain, Apple and other companies have made their devices virtually warrant-proof by enabling encryption by default and moving from four-digit passcodes to six.

"We have always maintained there is no such thing as a backdoor just for the good guys," Apple said last month, responding to Barr's claims that the company had not helped unlock the two iPhones recovered from the Pensacola shooter.

"Today, law enforcement has access to more data than ever before in history, so Americans do not have to choose between weakening encryption and solving investigations," Apple said. "We feel strongly encryption is vital to protecting our country and our users' data."

Cracking the codes

It looks like a bomb shelter. In a sense, it is.

Just off the main corridor of the Manhattan cyber laboratory, protected by a heavy steel door, is a small chamber where some of the lab's most consequential work is carried out in isolation.

About 100 locked cell phones, seized in various criminal investigations, are stacked neatly on two shelves. Nearby, computers silently batter the devices with spurts of numerals as they attempt to guess the passcodes.

Only when the lights are off is the work visible, in flashes of blinking lights.

Success can come in minutes, hours, days or months. Or not at all.

Of the 1,035 devices that were locked on arrival at the lab last year, 405 remain inaccessible, according to lab records. The year before, 666 of the 1,047 locked phones could not be opened.

New batches of phones are moved into the chamber like unbaked cookies. Others are moved out before they're done.

"We might need more shelving," said Steven Moran, director of the High Technology Analysis Unit.

The room's heavy drape of security, Moran said, is not for show. It was built to block outside radio frequencies, preventing suspects from remotely erasing their devices before examiners can break the locks.

"It is a real concern," Moran said, adding that some suspects released on bond have sought to do just that.

In particularly urgent cases, or when devices prove especially resistant, they are hand-delivered to private contractors who subject the phones to new types of hacking.

From 2014 to 2019, Vance said, his office paid those contractors $1.5 million for software and assistance.

Their help has become critical not only in Manhattan but in places like South Carolina's 14th Judicial Circuit, a five-county area in the state's low country where Duffie Stone is the local prosecutor.

"The use of technology by criminals is probably the biggest change in the criminal justice system," Stone said. "We are confronting this kind of technology, and the challenge of penetrating it, in virtually every case we are prosecuting."

Stone credits Vance with helping other prosecutors take on the new investigative burdens.

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

In 2018, Vance said, an internal survey revealed 17 cases in which his office "reduced or dismissed charges because of evidence recovered from a smartphone."

Barr and Vance: an unlikely alliance

Ordinarily, few would confuse William Barr with Cyrus Vance.

As Donald Trump's attorney general, Barr has shielded his boss from Vance's subpoenas and document requests. Their fight over the president's tax records is now before the Supreme Court.

On the issue of encryption, however, they have found common ground.

Last month, Barr rekindled a longstanding dispute between the Justice Department and Apple when he accused the company of failing to provide "substantive assistance" in unlocking two iPhones used by the Saudi attacker who killed three people at Naval Air Station Pensacola in December.

One of the devices was believed to have been damaged by a bullet fired by the gunman in an attempt to destroy any evidence it contained.

The attorney general said investigators rebuilt both phones, but they had not been able to bypass the passcodes to gain access to the data.

"This situation perfectly illustrates why it is critical that investigators be able to get access to digital evidence once they have obtained a court order based on probable cause," Barr said then.

Apple rejected Barr's rebuke, saying it had responded quickly to investigators' many requests. The company said it learned only a week earlier that the Justice Department needed help unlocking the phones.

FBI demanded Apple unlock iPhone of San Bernardino shooter

Barr's criticism mirrored a standoff between the FBI and Apple over an iPhone recovered after a 2015 mass shooting in San Bernardino, California, that left 14 people dead.

In that case, the FBI went to federal court to demand Apple assist investigators in accessing the device recovered from terrorist Syed Farook, who was killed with his wife, Tashfeen Malik, in a shootout with authorities following the attack.

The FBI's effort was led by then-director James Comey, who maintained the bureau wanted access only in that case. Apple and other tech companies feared granting access to Farook's phone would ultimately require them to build so-called backdoors that would allow law enforcement around the country to access their devices.

The FBI dropped its challenge after it secured the assistance of an outside contractor that successfully bypassed the iPhone's passcode.

Vance, who supported Comey's efforts at the time, said the San Bernardino case raised public awareness of the problem. But it ultimately "deflated because there was mutual finger-pointing."

If Barr were to challenge Apple again, Vance said he probably would support it. Yet the district attorney said courts won't offer a long-term solution.

"Nothing really has changed" since San Bernardino, Vance said.

"Companies are not going to redesign their devices to open for search warrants," he said. "The only way to move forward is the threat of federal legislation."