NYPD

New York City Police Department

PREPARED TESTIMONY OF
CHIEF OF INTELLIGENCE THOMAS P. GALATI
NEW YORK CITY POLICE DEPARTMENT

BEFORE THE HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
“Deciphering the Debate Over Encryption:
Industry and Law Enforcement Perspectives”

APRIL 19, 2016

Thank you to the committee for the opportunity to speak with you this morning.

Years ago, criminals and their accomplices stored their information in closets, drawers, safes, and glove boxes. There has been and continues to be an expectation of privacy in these areas, but the high burden imposed by the Fourth Amendment, which requires a lawful search be warranted and authorized by a neutral judge, has been deemed sufficient protection against unreasonable governmental search and seizure for the past 224 years. It now seems, however, that this legal authority is struggling to catch up with the times.

In today’s world, nearly everyone lives his or her life on a smartphone, and this includes criminals. Evidence that once would have been stored in a file cabinet or a notebook is now archived in an email or a text message. The same exact information that would solve a murder, catch a rapist, or prevent a mass shooting is now stored in that device. But where law enforcement has legal access to the file cabinet, it is shut out of the phone—not because of constraints inherent in the law, but because of limitations in accessibility imposed by technology.

When law enforcement is technologically unable to access evidence necessary to the investigation, prosecution, and prevention of crime, despite the lawful right to do so, we describe it with the term “going dark.” Every day, we deal with this evidentiary dilemma on two fronts.

First, there is what is known as “data at rest.” This is when the actual device—the computer, tablet, or phone—is in law enforcement’s possession, but the information stored within it is inaccessible.

In New York City, in just the six-month period from October, 2015 through March of this year, we have been locked out of 67 Apple devices lawfully seized pursuant to the investigation of 44 violent crimes. These incidents include 23 felonies, ten homicides, two rapes, and an instance in which two officers were shot in the line of duty. The incidents include robberies, criminal weapons possession, criminal sex acts, and felony assaults. In every case, we have the “file cabinet,” as it were, and the legal authority to open it, but we lack the technical ability to do so because encryption protects the contents of those 67 Apple devices. In every case, however, these crime victims deserve our protection.

The second type of “going dark” incident is known as “data in motion.” In these cases, law enforcement is legally permitted—through a warrant or other judicial order—to intercept and access a suspect’s communications. But the encryption built-in to applications such as “WhatsApp,” “Telegram,” “Wickr,” and others thwarts this type of lawful surveillance, because even if the information can be intercepted, it cannot be understood.

As a result, we may know a criminal group is communicating, but we are unable to understand why. In the past, a phone or wiretap—legally obtained through a judge—would alert the police to drop-off points, hide outs, and target locations. Now, we are literally in the dark. Criminals know it: we recently heard a defendant in a serious felony case make a telephone call from Riker's Island in which he extolled Apple's iOS 8 and its encryption software as "a gift from God."

This leaves the police, prosecutors, and the people we are sworn to protect in a very precarious position. What is even more alarming is that this position is not dictated by our elected officials, our judiciary system, or our laws. Instead, it is created and controlled by corporations like Apple and Google. These corporations have taken it upon themselves to decide who can access critical information in criminal investigations. As a Bureau Chief in our nation's largest municipal police department—an agency that is charged with protecting eight-and-a-half million residents and tens of millions of daily commuters and tourists every day—I am confident that corporate CEOs do not hold themselves to the same public-safety standard as our elected officials and law-enforcement professionals.

Given this, how do we keep people safe? The answer cannot be warrant-proof encryption, which creates a landscape of criminal information outside the reach of a search warrant or subpoena, as well as outside the legal authority established over centuries of jurisprudence.

Until 19 months ago, Apple agreed. Until 19 months ago, Apple held the key that could override protections and open phones. Apple used this "master key" to comply with court orders in drug, kidnapping, murder, and terrorism cases. There was no documented instance of this code getting out to hackers or to the government. If they were able to comply with constitutionally legal court orders then, why not now?

The ramifications of this fight extend beyond San Bernardino, California, and the 14 people murdered there. It is important to recognize that more than 90 percent of all criminal prosecutions in our country are handled at the state or local level. These cases involve real people—your families, your friends, and your loved ones. They deserve police departments that are able to do everything within the law to bring them justice, and they deserve corporations that appreciate their ethical responsibilities.

I applaud you for holding this hearing today. It is critical that we work together to fight crime and disorder, because criminals are not bound by jurisdictional boundaries nor industry standards. They are increasingly aware of the safety net that warrant-proof encryption provides them, however, and we must all take responsibility for what that means. For the New York City Police Department, it means investing more in people's lives than in quarterly earnings reports, and putting public safety back into the hands of the brave men and women who have sworn to defend it.

I would be happy to answer any questions.