Department of Justice

STATEMENT OF

AMY HESS
EXECUTIVE ASSISTANT DIRECTOR
SCIENCE AND TECHNOLOGY BRANCH
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATION
COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"DECIPHERING THE DEBATE OVER ENCRYPTION: INDUSTRY AND LAW ENFORCEMENT PERSPECTIVES"

PRESENTED

APRIL 19, 2016

Statement of
Amy Hess
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation

Before the
Subcommittee on Oversight and Investigation
Committee on Energy and Commerce
U.S. House of Representatives

At a Hearing Entitled
"Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives"

Presented
April 19, 2016

Good morning, Chairman Murphy, Ranking Member DeGette, and members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the ongoing challenges encryption presents to law enforcement's ability to obtain electronic information and evidence pursuant to a court order or warrant.

In recent years, new methods of electronic communication have transformed our society, most notably by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security. We have benefited immensely from digital communication and e-commerce, but with those conveniences come risks and dangers, and we have seen how criminals, including terrorists, also use advances in technology to their advantage. We as a nation are faced with trying to maximize privacy and security, both of which we value as a society.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance — not simply because the Constitution demands it — but because the free flow of information is vital to a thriving democracy.

We also have always investigated and prosecuted those wishing to do harm to our nation and its people. As national security and criminal threats continue to evolve, the FBI must continue to work hard to stay ahead of changing threats and changing technology. The more we as a society rely on electronic devices to communicate and store information, the more likely it is

that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case — from homicides and kidnappings, to drug trafficking, financial fraud, trade secret theft, and child exploitation — where critical evidence came from smart phones, computers, and online communications. Increasingly, some technologies are prohibiting law enforcement from having access to that critical evidence.

The problem, at its base, is one of choices about how to maximize privacy and security to the greatest extent possible. We are not asking to expand the Government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress provided to us to keep America safe. There is not, and will not be, a single solution to address the variety of challenges we face. The FBI is pursuing multiple avenues to overcome these challenges; however, it is clear that we cannot overcome these challenges on our own.

For example, one potential approach involves the exploitation of vulnerabilities previously unknown to the device or software manufacturer in order to gain access to information contained within or protected by it. While this is possible in some instances, it is often not a viable solution for law enforcement. Identifying these vulnerabilities and developing lawful intercept or lawful access solutions can take an unacceptable amount of time, require significant skill and resources, and the results of these efforts can be ephemeral, at best.

In order to better protect this nation and its people from harm, we need to be able to access electronic information. When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to root out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to identify and stop terrorists who are using social media to recruit, plan and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence. These are not just theoretical concerns.

Malicious actors have taken advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information.

Terrorist groups, such as ISIL, also use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. Some of these conversations occur over publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

We have decisions to make, with our government partners, industry, and the American people. We must find solutions to ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds legally sufficient reason to believe that certain private communications contain evidence of a crime, then the Government can conduct a limited search for that evidence. For example, by having a neutral arbiter — the judge — evaluate whether the Government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' constitutional rights.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the FBI fully complies with those protections. The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime or intelligence that might prevent an attack?

The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently implemented poses real barriers to law enforcement's ability to seek information in authorized investigations. Mr. Chairman, we believe that the challenges posed by this problem are grave, growing, and extremely complex. At the outset, it is important to emphasize again that we believe there is no one-size-fits-all strategy that will ensure success. We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe.