**STATEMENT OF**

**KENNETH L. WAINSTEIN**

**PARTNER, CADWALADER, WICKERSHAM & TAFT LLP**

**CONCERNING**

**CYBERSECURITY AND U.S. NATIONAL SECURITY**

**BEFORE THE**

**COMMITTEE ON ARMED SERVICES**

**UNITED STATES SENATE**

**JULY 14, 2016**

Chairman McCain, Ranking Member Reed, and distinguished Members of the Committee, thank you for the invitation to appear before you today. My name is Ken Wainstein. I am a partner at the law firm of Cadwalader, Wickersham & Taft, and I previously served as the Homeland Security Advisor to President George W. Bush, as the Assistant Attorney General for National Security, and in a variety of other positions in the Justice Department. Thank you for the opportunity to address the pressing national security issues raised by encryption.

## I. Introduction

We are in the midst of a national debate that was triggered by the recent adoption of default encryption by large communications service providers. The debate is between those in government who insist there should be a technical accommodation allowing them to penetrate encryption and surveil criminal and terrorist communications and those in the technology and civil liberties communities who insist that any such accommodation would compromise encryption and jeopardize the security of our communications. This debate has been going on for

about two years, and we now find ourselves at an impasse with neither side showing any sign of backing down.

It is time for Congress to step in and break through that impasse. Congress has long played a pivotal role in striking the balance between individual and societal privacy interests and our government's law enforcement and national security interests. Congress should play that role once again by pushing both sides of this debate toward a solution to this impasse.

## II. Legal Background

Since the dawn of telephony, we have wrestled with the question of when and under what conditions government investigators should be allowed access to the content of private communications. In the 1967 decision *Katz v. United States*, the Supreme Court ruled that an individual has a reasonable expectation of privacy in the content of his or her phone calls, and the next year Congress passed Title III of the Omnibus Crime Control and Safe Streets Act, mandating the process by which the government must make a probable-cause showing to secure a judicial warrant authorizing it to use a wiretap. After Congressional investigations in the 1970's revealed a series of surveillance abuses against persons like Dr. Martin Luther King, Jr., Congress passed the Foreign Intelligence Surveillance Act of 1978 ("FISA") creating a process of judicial review and approval for electronic surveillance to obtain information related to foreign intelligence, international terrorism, foreign espionage and other national security threats.

With the passage of Title III and FISA, Congress struck a balance between the privacy interests in electronic communications and the legitimate needs of law enforcement and intelligence agencies to obtain access to those communications. While the balance Congress struck in each of these laws—and other laws addressing government investigative access to private information—may have been suitable at that time, that balance shifted with the evolution of technology in the ensuing years, which, in turn, triggered a series of national debates over how best to adapt existing laws to new technological realities. Over the past couple decades, Congress has done a very commendable job of brokering those debates and bringing the surveillance laws up to date. No better example was the legislative debate in 2007-08 that resulted in the FISA Amendments Act, a well-considered piece of legislation that realigned our foreign intelligence surveillance authorities to account for the revolution in communications technology since the passage of FISA in 1978.

Once each of those debates was resolved and the rules were legislatively established, government officials could then move forward to conduct the surveillance they needed. To get the judicial authorization, they provided the required predication and justification to the relevant court and received the court's authorizing warrant or order. Then, to get the warrant or order implemented, they served the relevant communications provider with a secondary order commanding the provider to execute the warrant or order.

## III. Going Dark

Over time, however, this process became less and less reliable as more and more providers were unable to give the government the assistance necessary to execute the authorized surveillances. With the exponential increase in the volume of electronic communications and the diversification of technologies from wire telephony to mobile voice communications over digital, switch-based services, many providers became either unable or unwilling to satisfy lawful wiretap requests. As a result, by the mid-1990's, law enforcement agencies saw that their surveillance capabilities were declining, and they started to worry that they were "going dark."

Congress responded to this concern in 1994 by passing the Communications Assistance for Law Enforcement Act ("CALEA"), which required telecommunications carriers to modify their equipment, facilities, and services to ensure that the government could conduct lawfully-authorized surveillances.

Despite CALEA, significant gaps remained in our surveillance capabilities. There were a number of companies that simply did not invest the money and time necessary to develop the capabilities to enable surveillance in their systems. In addition, there developed a broad range of communications technologies—like email, instant messaging, social networking sites and peer-to-peer services—that were simply not covered by CALEA. As a result, the government was increasingly unable to surveil its criminal and national security targets by the end of the last decade.

This "going dark" issue then became exponentially more problematic with the recent advent of default endpoint and end-to-end encryption. With endpoint encryption, the data is encrypted while stored on the communication device, while with end-to-end encryption, the contents of a communication are encrypted in transit. In both scenarios, the service provider and device manufacturer have limited access, if any, to the encryption key, which is typically held by the device owner or stored on the device. Endpoint and end-to-end encryption became the default settings for a large number of devices and services when Apple unveiled a new operating system for its iPhones and other devices in September 2014, and other service providers like Google followed suit for certain device and service offerings. As a result of these default encryption processes, service providers and device manufacturers are often unable to satisfy lawful court surveillance orders—a scenario that will increasingly put our law enforcement and national security officials in the dark as this technology becomes industry standard and our adversaries gravitate to it.

## IV. Going Dark Going Forward

This dilemma is now clear for all to see, and the battle lines have been drawn, with the government and tech industry taking dueling views on the way to proceed. FBI Director James Comey has argued that the increasing availability and use of endpoint and end-to-end encryption puts our country at grave risk, as it effectively creates safe spaces for criminals and terrorists to

operate outside the reach of law enforcement or the Intelligence Community. He acknowledges the important privacy interests at stake, but asserts that those interests must be balanced with the security interests of the broader society and urges industry to search for a technological solution that can accommodate the government's lawful surveillance needs.

Representatives of the tech industry and the civil liberties community have aggressively countered Director Comey's position with a variety of arguments, including the following:

- That any accommodation for the government would introduce a vulnerability that would undermine the security and integrity of encryption, which inarguably is a vitally important technology for protecting information and preventing theft and other cyber mischief;

- That any such accommodation could not be confined to the United States, as other governments—including repressive governments—would likely demand the same access;

- That any accommodation would put U.S. tech companies at a competitive disadvantage because customers—especially overseas customers and those who are already suspicious of U.S. government surveillance in the aftermath of the Snowden revelations—may stop using those companies' services if they learn that the companies are cooperating with the U.S. government to circumvent encryption; and

- That any accommodation imposed on U.S. companies would be of limited effectiveness because criminals, terrorists and other wrongdoers would simply start using foreign encrypted services.

Citing these arguments, some in the tech industry and civil liberties community have taken an absolutist position that there should be no government accommodation at all. One tech industry association sent President Obama a letter urging him to resist "encryption 'work-arounds'" for the government's surveillance needs, contending that a work-around would "compromise the security of [communications] products and services, rendering them more vulnerable to attacks and [] erode consumers' trust in the products and services they rely on for protecting their information."

I fully appreciate the importance and tremendous societal value of strong encryption, and I recognize the validity of the tech industry's concerns. However, I do not believe that those concerns automatically mean that encryption should be inviolable and that our government should henceforth be denied access to large swaths of communications. That reasoning just does not square with the reality of today's national security imperatives.

That reality is that government access to these communications is critical to our national security. From my earliest days as a federal prosecutor investigating narcotics networks, I saw the value of communications surveillance in gaining insight into the plans and inner workings of

a conspiracy. That value is particularly high when the conspiracy being investigated is a foreign terrorist group, where leaders and foot soldiers are often located in different parts of the world and have to rely on electronic communication for operational coordination.

Thanks in large part to our signals intelligence capabilities, the government has been fairly successful in detecting and protecting our country against large-scale terrorism since 9/11. That record of success is now being tested, however, by the rise of ISIS, which in many ways is a more formidable adversary than al-Qaeda ever was. In response to our allies' recent success in pushing back the borders of its conquered territory, ISIS seems determined to counter those losses with terrorist attacks directed against the homelands of those countries—like the U.S.—that they consider their mortal enemies.

It is also clear that ISIS recognizes the operational value of encrypted communications. We know that it has issued a guide for its members discussing the relative "safety" of different encrypted messaging apps. We know that as part of its recruiting efforts, ISIS often initially engages on social media, but then moves the conversation to encrypted apps. And, we know that attackers inspired by ISIS have made use of such apps prior to conducting their attacks. For example, FBI Director Comey has testified that one of the attackers at the Muhammad art exhibit in Garland, Texas exchanged over 100 encrypted messages with a known overseas terrorist on the morning of the shooting. Those messages remain encrypted and unreadable by investigators.

## V. Resolving the Debate

With this gathering threat on the horizon, now is not the time to blithely concede that encryption automatically trumps surveillance and allow our intelligence and law enforcement agencies to go dark. To the contrary, now is the time for Congress to mobilize on this issue and push for a solution—a solution that allows government the access it needs to protect our people and our country without unduly compromising the encryption technology that protects our data and communications.

I urge Congress to embark on a legislative process that calls on both sides of this debate to fully lay out the basis of their views:

- For the government, this means laying out the case that concretely demonstrates how significantly their different investigative efforts are—or are not—handicapped by the use of default encryption technologies.

- For the tech industry and civil liberties groups, this means laying out technically specific support for the contention that a government accommodation would undermine the integrity of default encryption. They should provide hard data that demonstrates exactly how—and how much—each possible type of accommodation would impact their encryption systems. It is only when Congress receives that data that it can knowledgeably perform its deliberative function and balance the potential cyber security dangers posed

by a government accommodation against the national security and law enforcement benefits of having such an accommodation in place.

Congress can undertake this effort either through a series of hearings and a traditional legislative process, or else through the establishment of a commission like that proposed by Senator Warner and Chairman McCaul—a commission composed of technologists, security experts and other key stakeholders who could delve deeply into the intricacies of this complex issue.

Either of these options would be a significant step forward. The option that is <u>not</u> a step forward is the option of inaction and continued impasse. We have seen the consequences of that option before, as that was the option the government effectively pursued in the late 1990's and early 2000's when debating the wisdom of "the wall," the regulatory barrier that prevented coordination and information sharing between law enforcement and Intelligence Community personnel. That inaction had tragic consequences when the existence of the wall contributed to our inability to identify the 9/11 hijackers and prevent them from launching their attacks.

Congress dismantled the wall when it passed the PATRIOT Act six weeks after the 9/11 attacks, but that was too late for the 3,000 murdered Americans. We made the mistake of inaction once before; we must not make it again.

I applaud the Committee for holding today's hearing and showing leadership on this issue. It gives me hope that we can, in fact, move beyond the current impasse and reach a workable solution to this critical problem. My thanks again for inviting me, and I look forward to answering any questions you may have.