JUSTICE NEWS

Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy

Annapolis, MD ~ Tuesday, October 10, 2017

Remarks as prepared for delivery

Thank you, Professor Kosseff, for that kind introduction. I am honored to be here today with some of our nation's finest public servants.

We meet today just over a mile from Navy-Marine Corps Memorial Stadium, where the Navy pulled off an epic victory three days ago against the Air Force. After the highest-scoring game in the rivalry's 50-year history, the Midshipmen scored a go-ahead touchdown just seconds before the final whistle. The Navy's commandant, Robert B. Chadwick II, said that "when you play someone with the same DNA as you, you know they aren't going to quit either."

The game is a reminder that victory frequently requires ceaseless determination.

The Navy has a long history of determination, and of fearless exploration. The Center for Cyber Security Studies stands well within that tradition of embracing the unknown in defense of the nation. But for all its dynamism, the Navy is built on continuity. Our Navy traces its history to the Continental Navy established during the Revolutionary War. The core mission of defending liberty has remained constant across generations.

Each Midshipman swears to "support and defend the Constitution of the United States against all enemies, foreign and domestic." Our federal prosecutors take the same oath.

An oath is meant to be serious business. The oath-taker promises to live by certain rules in return for a privilege bestowed by the government.

There was a time when taking an oath was a matter of life and death. Sir Thomas More was an Englishman who was executed in 1534 because he refused to swear an oath to King Henry VIII. In Robert Bolt's play based on More's life, More tells his daughter, "When a man takes an oath … he's holding his own self in his hands. Like water. And if he opens his fingers then — he needn't hope to find himself again."

Your oath carries a solemn obligation. It obliges you to preserve our nation's commitment to the rule of law.

The words require you to honor that commitment not only when it is easy, but when it is difficult.

In 1776, during the Revolutionary War, Thomas Paine wrote, "The summer soldier and the sunshine patriot will, in … crisis, shrink from the service of [their] country." Paine recognized that it is easy to claim the mantle of patriotism when the winds are peaceful and the seas are calm. True patriots are the ones who remain at their posts during the storm.

In 1864, almost a century after the founding of our nation, Admiral David Farragut watched his fleet pause as it approached Mobile Bay, Alabama. Farragut asked why the ships were hesitating. The answer came back, "Torpedoes!" Farragut then uttered the immortal reply, recorded by history as "Damn the torpedoes, full speed ahead!"

Sometimes we face real torpedoes. And sometimes, in the cyber world, we face virtual torpedoes. Whatever the challenges ahead, we are duty-bound to sustain our timeless rule of law values in an era of disruptive technological

change.

Defending the rule of law is essential because the rule of law is not just a feature of the United States. It is the foundation of the United States. To use a technological metaphor, the rule of law is our nation's operating system.

The rule of law means that our nation is governed by principles that are agreed to in advance. Government officials are required to obey and enforce the rules, and restricted from making arbitrary decisions unsupported by the rules.

We should never take the rule of law for granted. We learned this spring about the tragic experience of Otto Warmbier, the University of Virginia college student who allegedly took a poster off a hotel wall in North Korea and was sentenced to 15 years of hard labor. North Korea sent Otto home 17 months later. They sent him home with brain damage. He died a few days later.

North Korea will not hold anyone accountable for Otto's injuries and death. It is a totalitarian government with no concept of the rule of law. No civil rights. No due process. No justice.

The North Korean government offered no explanation and no apology for prohibiting all communication and concealing Otto's condition from his family.

My teenage daughter could not believe that such an evil place exists in the 21st century.

Sometimes people get so caught up complaining about the imperfections in our own system that they fail to appreciate how fortunate we are to live in a country blessed with officials who obey the rules and protect the innocent. People who sail towards danger so the rest of us can stay safe. People like you.

Protecting people from abuse by the government is an important aspect of the rule of law. But the rule of law also protects people from being victimized by other people.

The preamble to the United States Constitution explains that it aims to "establish justice, insure domestic tranquility, provide for the common defence, promote the general welfare, and secure the blessings of liberty…."

Our social contract empowers the government to protect society from criminals. The Congress defines federal crimes and authorizes tools for investigating them, such as subpoenas, search warrants, and wiretaps.

Those legal authorities enable investigators and prosecutors to gather the evidence needed to enforce the laws. Evidence is essential because our legal system protects criminal defendants by requiring the prosecution to produce admissible evidence that establishes their guilt beyond any reasonable doubt.

But increasingly, the tools we use to collect evidence run up against technology that is designed to defeat them.

Technological dynamism has profoundly transformed our society in recent years. Ninety-five percent of Americans own a cell phone and more than three-quarters of us own a smartphone. Nearly seven in ten Americans use social media. In 2014, the Internet sector was responsible for an estimated $922 billion, or six percent of the U.S. real GDP — and that figure is rising.

Our lives are increasingly dependent on a growing digital infrastructure. But much of that infrastructure is being targeted by criminals and foreign adversaries. Since 2012, the U.S. Intelligence Community's Worldwide Threat Assessment has frequently listed the cyber threat as a major danger to our nation's security.

In May, medical facilities around the world were attacked with ransomware, resulting in the cancellation of medical procedures, the unavailability of patient records, and the diversion of ambulances. In March 2016, hospitals here in Maryland were hit by a ransomware attack, forcing patients to be turned away or treated without updated computer records. Another alarming incident occurred in 2013, when a foreign adversary gained access to the control and data acquisition system for a dam in New York. Fortunately, the dam's sluice gate, which controls water levels and flow

rates, had been disconnected for maintenance. Otherwise, our adversary might have been able to remotely operate the gate.

At the Department of Justice, we take such threats extremely seriously and view countering them as one of our highest priorities. We aggressively investigate, indict, and — when possible —prosecute the cybercriminals and foreign state hackers behind such attacks. We create novel partnerships within the federal government to use an "all tools" approach. If prosecution is not the most appropriate course of action, we work with partners in other agencies to pursue the most effective alternatives.

Private sector entities are crucial partners in this fight. We engage in formal and informal information sharing, promote cybersecurity best practices, and make clear that private sector cyber victims will be treated with respect and concern.

But our effectiveness, and those of our governmental partners, has limits. The digital infrastructure is not always constructed with adequate regard for public safety, cybersecurity, and consumer privacy.

Unless we overcome those complications, we will remain vulnerable.

In 2016, an attack launched against domain name servers illustrated a significant problem. The attack made it effectively impossible for many users to access certain web sites for several hours. The attackers took control of multiple computers on the Internet and used them to conduct a distributed denial of service attack. What made the attack especially worrisome was that it used simple internet-connected devices, such as cameras and digital video recorders. Those so-called "Internet of Things" devices surround us, and they are easily susceptible to control by hackers because of the widespread use of default passwords and other failures to secure them.

That incident vividly illustrates that our digital infrastructure is not just a target in a traditional sense. It can be hijacked and used against us as an attack vector. The possibilities for such attacks will grow. Estimates reveal that 6.3 billion internet-connected devices were used in 2016. The total may reach 20.4 billion by 2020. Imagine the possible attack vectors if all of those devices employed default passwords.

One of our principal challenges today is the threat that new technologies pose to our individual and collective security. Those technologies can play a critical role in creating jobs, promoting commerce, and enhancing our lives. But new technologies will pose new dangers if innovations develop so quickly that the laws cannot keep up with them.

Our challenge extends far beyond the new technologies that our adversaries use to conduct new types of attacks. Our investigators and prosecutors already face a range of cyber issues that undermine the rule of law.

Consider, for instance, how the "dark web" facilitates child exploitation and promotes trade in illicit goods. Or consider how criminals take advantage of new technology that conceals their identities to commit crimes such as trading child pornography and making bomb threats.

Our investigators face challenges because data can be dispersed and evanescent. Communications providers often choose to store data overseas, which sometimes results in American law enforcement being unable to access evidence involving American perpetrators who violate American laws and harm American victims. We also face lengthy delays because some domestic technology providers do not design their systems to facilitate responses to court orders, and some do not adequately staff their legal compliance departments.

That brings me to one of our greatest challenges, encryption. Encryption is a foundational element of data security and authentication. It is essential to the growth and flourishing of the digital economy, and we in law enforcement have no desire to undermine it.

But the advent of "warrant-proof" encryption is a serious problem. Under our Constitution, when crime is afoot, impartial judges are charged with balancing a citizen's reasonable expectation of privacy against the interests of law enforcement. The law recognizes that legitimate law enforcement needs can outweigh personal privacy concerns.

Our society has never had a system where evidence of criminal wrongdoing was totally impervious to detection, especially when officers obtain a court-authorized warrant. But that is the world that technology companies are creating.

Those companies create jobs, design valuable products, and innovate in amazing ways. But there has never been a right to absolute privacy. Courts weigh privacy against other values, including the need to solve and prevent crimes. Under the Fourth Amendment, communications may be intercepted and locked devices may be opened if they are used to commit crimes, provided that the government demonstrates showing of probable cause.

Warrant-proof encryption defeats the constitutional balance by elevating privacy above public safety. Encrypted communications that cannot be intercepted and locked devices that cannot be opened are law-free zones that permit criminals and terrorists to operate without detection by police and without accountability by judges and juries.

When encryption is designed with no means of lawful access, it allows terrorists, drug dealers, child molesters, fraudsters, and other criminals to hide incriminating evidence. Mass-market products and services incorporating warrant-proof encryption are now the norm. Many instant-messaging services employ default encryption designs that offer police no way to read them, even if an impartial judge issues a court order. The makers of smart phones previously kept the ability to access some data on phones, when ordered by a court to do so. Now they engineer away even that capability.

We refer to this problem as "Going Dark" – the threat to public safety that occurs when service providers, device manufacturers, and application developers deprive law enforcement and national security investigators of crucial investigative tools.

The issue caught the public's attention in February 2016, when the government obtained an iPhone used by a terrorist who shot and killed 14 people and injured 22 others at an office Christmas party in San Bernardino, California. The FBI wanted to find out if the phone contained evidence of other attack plans, or information about other people who might launch attacks. So, the FBI obtained the consent of the phone's legal owner—the San Bernardino county government —and also obtained a search warrant. The data on the phone was encrypted, but Apple had the ability to assist the government in obtaining that data. The government sought Apple's voluntary assistance.

Apple rejected the government's request, although it had the technical capability to help. The government then obtained a court order requiring Apple to assist, but Apple immediately announced it would appeal the order. Fortunately, the government was able to access data on that iPhone without Apple's assistance.

But the problem persists. Today, thousands of seized devices sit in storage, impervious to search warrants. Over the past year, the FBI was unable to access about ** mobile devices submitted to its Computer Analysis and Response Team, even though there was legal authority to do so.

In May 2015, terrorists targeted people attending an event in Garland, Texas. On the morning of the attack, one of the terrorists exchanged 109 instant messages with an overseas terrorist. He used an app employing end-to-end encryption, so that law enforcement could not decode the messages.

Billions of instant messages are sent and received each day using mainstream apps employing default end-to-end encryption. The app creators do something that the law does not allow telephone carriers to do: they exempt themselves from complying with court orders.

Responsible encryption is achievable. Responsible encryption can involve effective, secure encryption that allows access only with judicial authorization. Such encryption already exists. Examples include the central management of security keys and operating system updates; the scanning of content, like your e-mails, for advertising purposes; the simulcast of messages to multiple destinations at once; and key recovery when a user forgets the password to decrypt a laptop.

No one calls any of those functions a "back door." In fact, those capabilities are marketed and sought out by many

users.

The proposal that providers retain the capability to make sure evidence of crime can be accessed when appropriate is not an unprecedented idea.

Such a proposal would not require every company to implement the same type of solution. The government need not require the use of a particular chip or algorithm, or require any particular key management technique or escrow. The law need not mandate any particular means in order to achieve the crucial end: when a court issues a search warrant or wiretap order to collect evidence of crime, the provider should be able to help.

No law can guarantee that every single product that offers encryption will also come with an adequate capability to prevent that product from being used to hide evidence of crime.

A requirement to implement a solution could be applied thoughtfully, in the places where it is needed most. Encrypted communications and devices pose the greatest threat to public safety when they are part of mass-market consumer devices and services that enable warrant-proof encryption by default.

No solution will be perfect. If only major providers refrain from making their products safe for terrorists and criminals, some sophisticated criminals may migrate to less-used platforms. But any progress in preserving access to communications methods used by most criminals and terrorists would still be a major step forward.

The approach taken in the recent past — negotiating with technology companies and hoping that they eventually will assist law enforcement out of a sense of civic duty — is unlikely to work. Technology companies operate in a highly competitive environment. Even companies that really want to help must consider the consequences. Competitors will always try to attract customers by promising stronger encryption.

That explains why the government's efforts to engage with technology giants on encryption generally do not bear fruit. Company leaders may be willing to meet, but often they respond by criticizing the government and promising stronger encryption.

Of course they do. They are in the business of selling products and making money.

We use a different measure of success. We are in the business of preventing crime and saving lives.

Companies are willing to make accommodations when required by the government. Recent media reports suggest that a major American technology company developed a tool to suppress online posts in certain geographic areas in order to embrace a foreign government's censorship policies. Another major American tech company recently acquiesced to a foreign partner's request that local customers stop using software to circumvent a foreign government's censorship restrictions. A third major American corporation recently stopped supporting virtual private network apps at the behest of a foreign government, to prevent internet users from overcoming censorship policies.

American technology providers sell products and services in foreign markets where the governments have questionable human rights records and enforce laws affording them access to customer data, without American due process or legal protections.

Surely those same companies and their engineers could help American law enforcement officers enforce court orders issued by American judges, pursuant to American rule of law principles.

Some critics argue that the evidence concealed by encryption can be offset by new sources of data. They claim we live in a "Golden Age of Surveillance" because law enforcement may access new sources of information such as location data, or data derived from internet-connected devices.

That argument misunderstands what sort of evidence law enforcement needs in order to prevent and punish crime. We need to assemble powerful evidence that proves a defendant's guilt beyond a reasonable doubt. Sometimes a

communication is a crime in itself, or provides conclusive proof. There is no substitute for introducing the original communication in court.

Location data may demonstrate that a suspect was near the scene of crime, but it does not necessarily prove that the person committed a crime. Nor does it show what the suspect was thinking or intending — both of which are important elements of proof in many prosecutions.

It is notable that all of the new data is generated for, and in the hands of, private companies. Companies collect increasing volumes of personal information about individuals in order to predict human behavior and produce revenue. Databases are built for marketers, who are comfortable making decisions based on far less information and far less assurance of accuracy than we require before prosecuting someone for a crime.

We may be awash in data, but it is not always the kind of evidence that our rule of law tradition establishes as sufficient to establish guilt beyond any reasonable doubt.

Police and prosecutors were the first to recognize the danger posed by the "going dark" trend. But the public bears the cost. When investigations of violent criminal organizations come to a halt because we cannot access a phone, lives may be lost. When child molesters can operate anonymously over the internet, children may be exploited. When terrorists can communicate covertly without fear of detection, chaos may follow.

It is important to recognize that our concern about the harm caused by "going dark" is not inconsistent with our support for cybersecurity. We at the Department of Justice understand and encourage strong cybersecurity to protect our citizens.

We know from experience that the largest companies have the resources to do what is necessary to promote cybersecurity while protecting public safety. A major hardware provider, for example, reportedly maintains private keys that it can use to sign software updates for each of its devices. That would present a huge potential security problem, if those keys were to leak. But they do not leak, because the company knows how to protect what is important. Companies can protect their ability to respond to lawful court orders with equal diligence.

Technology providers are working to build a world with armies of drones and fleets of driverless cars, a future of artificial intelligence and augmented reality. Surely such companies could design consumer products that provide data security while permitting lawful access with court approval.

As the "going dark" trend grows, local, state, and federal law enforcement officials need to be candid about how criminals use encrypted services and devices for illegal purposes.

In an era of dramatic and rapid change, we have a duty to maintain our commitment to the rule of law. That requires us to be forthcoming about the dangers posed by emerging threats.

If companies are permitted to create law-free zones for their customers, citizens should understand the consequences. When police cannot access evidence, crime cannot be solved. Criminals cannot be stopped and punished.

There is an alternative. Responsible encryption can protect privacy and promote security without forfeiting access for legitimate law enforcement needs supported by judicial approval.

Technology companies almost certainly will not develop responsible encryption if left to their own devices. Competition will fuel a mindset that leads them to produce products that are more and more impregnable. That will give criminals and terrorists more opportunities to cause harm with impunity.

Sounding the alarm about the dark side of technology is not popular. Everyone who speaks candidly about "going dark" faces attacks by advocates of absolute privacy.

Some advocates are motivated by profit. Others demonstrate sincere concern about the benefits of privacy. They are

not concerned about preserving law enforcement capabilities.

Those of us who swear to protect the rule of law have a different motivation. We are obliged to speak the truth.

The truth is that “going dark” threatens to disable law enforcement and enable criminals and terrorists to operate with impunity.

Allow me to conclude with this thought: There is no constitutional right to sell warrant-proof encryption. If our society chooses to let businesses sell technologies that shield evidence even from court orders, it should be a fully-informed decision.

Thank you for your attention, and thank you for your devoted service to our great nation. I look forward to your questions.

** Due to an error in the FBI's methodology, an earlier version of this speech incorrectly stated that the FBI had been unable to access 7,800 devices. The correct number will be substantially lower.

Speaker:
Deputy Attorney General Rod J. Rosenstein

Topic(s):
Cyber Crime

Component(s):
Office of the Deputy Attorney General

Updated May 23, 2018