CHRON

Department of Justice

STATEMENT OF

AMY HESS
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

CONCERNING

ENCRYPTION AND CYBERSECURITY FOR
MOBILE ELECTRONIC COMMUNICATION DEVICES

PRESENTED

APRIL 29, 2015

Statement of
Amy Hess
Executive Assistant Director
Federal Bureau of Investigation

Before the
Subcommittee on Information Technology
Oversight and Government Reform
U.S. House of Representatives

Concerning
Encryption and Cybersecurity for
Mobile Electronic Communication Devices

Presented
April 29, 2015

Good morning/afternoon, Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee. Thank you for the opportunity to appear before the Committee today, and for your continued support of the men and women of the FBI.

Today's FBI

As you know, the Bureau has undergone unprecedented transformation in recent years to address and prevent threats to our national security and our public safety, from terrorism, state-sponsored espionage, and cyber security to violent gangs, transnational organized crime, and crimes against children.

As national security and criminal threats continue to evolve, so too must the FBI evolve to stay ahead of changing threats and changing technology. Today's FBI is a threat-focused, intelligence-driven organization. We must continually ask ourselves whether we are able to meet the challenges of the day, whatever they may be.

Online technology has forever changed the world we live in. We're online, in one form or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. With this online presence comes the need to protect our privacy and the security of our data.

But, as with any technology, it can be used by some very dangerous people, and the FBI has a sworn duty to keep every American safe from crime and terrorism while simultaneously protecting their constitutional rights and preserving their civil liberties. Moreover, we recognize

our national interests in promoting innovation and the competiveness of U.S. companies in the global marketplace, as well as freedom of expression around the world.

The evolution of technology is creating new challenges for law enforcement and our ability to access communications. We call it "Going Dark," and it means that those charged with protecting the American people aren't always able to access the information necessary to prosecute criminals and prevent terrorism even though we have lawful authority to do so. To be clear, we obtain the proper legal authority to intercept and access communications and information, but we increasingly lack the technical ability to do so. This problem is broader and more extensive than just encryption. But, for purposes of my testimony today, I will focus on the challenges we face based on the evolving use of encryption.

The issues law enforcement encounters with encryption occur in two overlapping contexts. The first concerns legally authorized real-time interception of what we call "data in motion," such as phone calls, email, text messages and chat sessions in transit. The second challenge concerns legally authorized access to data stored on devices, such as email, text messages, photos, and videos – or what we call "data at rest." Both data in motion and data at rest are increasingly encrypted.

Court-Ordered Interception of Encrypted Data in Motion

In the past, there were a limited number of communications carriers. As a result, conducting electronic surveillance was more straightforward. We identified a target phone being used by a suspected criminal, obtained a court order for a wiretap, and, under the supervision of a judge, collected the evidence we needed for prosecution.

Today, communications occur across countless providers, networks, and devices. We take our laptops, smart phones, and tablets to work and to school, from the soccer field to the coffee shop, traversing many networks, using any number of applications. And so, too, do those conspiring to harm us. They use the same devices, the same networks, and the same applications to make plans, to target victims, and to concoct cover-up stories.

Law enforcement and national security investigators need to be able to access communications and information to obtain the evidence necessary to prevent crime and bring criminals to justice in a court of law. We do so pursuant to the rule of law, with clear guidance and strict judicial oversight. But increasingly, even armed with a court order based on probable cause, we are too often unable to access potential evidence.

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers to be able to implement court orders for the purpose of intercepting

communications. But that law wasn't designed to cover many of the new means of communication that exist today. Currently, thousands of companies provide some form of communication service, but most do not have the ability to isolate and deliver particular information when ordered to do so by a court. Some have argued that access to metadata about these communications – which is not encrypted – should be sufficient for law enforcement. But metadata is incomplete information, and can be is difficult to analyze when time is of the essence. It can take days to parse metadata into readable form, and additional time to correlate and analyze the data to obtain meaningful and actionable information.

Court-Ordered Access to Stored Encrypted Data

Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks.

In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default – without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice.

Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection.

Additional Considerations

Some assert that although more and more devices are encrypted, users back-up and store much of their data in "the cloud," and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many

companies impose fees to store information there – fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves – devices which are increasingly encrypted.

Facing the Challenge

The reality is that cyber adversaries will exploit any vulnerability they find. But security risks are better addressed by developing solutions during the design phase of a specific product or service, rather than resorting to a patchwork solution when law enforcement presents the company with a court order after the product or service has been deployed.

To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data. We have been on the front lines of the fight against cybercrime and economic espionage and we recognize that absolute security does not exist in either the physical or digital world. Any lawful intercept or access solution should be designed to minimize its impact upon the overall security. But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets.

A common misperception is that we can simply break into a device using a "brute force" attack – the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today's high-level encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the device to produce the information in a readable form?" Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court's order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography.

Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our

neighborhoods, and terrorists who may be 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 can't provide us with the password, especially when time is of the essence.

Examples

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that evidence that was once found in filing cabinets, letters, and photo albums will now be available only in electronic storage. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications.

Each of the following examples demonstrates how important information stored on electronic devices can be to prosecuting criminals and stopping crime. As encryption solutions become increasingly inaccessible for law enforcement, it is cases like these that could go unsolved, and criminals like these that could go free.

As an example of the importance of lawful access to smart phones, consider the case involving a long-haul trucker who kidnapped his girlfriend, imprisoned her within his truck, drove her from State to State, and physically and sexually assaulted her along the way. The victim eventually leapt from the truck and escaped to nearby civilians, and later the police. The trucker refuted the charges and claimed the sexual activity was consensual. In this case, law enforcement obtained a search warrant for the trucker's smart phone, as well as a court order requiring the phone manufacturer's assistance to extract that data. Through this court-authorized process, law enforcement recovered video and images of the abuse stored on the smart phone, which were integral to corroborating the victim's testimony at trial. The trucker was convicted of kidnapping and interstate domestic violence at trial, and sentenced to life in prison.

Additionally, in a case investigated by a small Midwest police department, a woman reported that an unknown stranger forcibly raped her while she was out walking. She sought treatment at a local hospital where a sexual assault examination was performed. However, the investigator noted peculiarities in the woman's responses during the interview and requested access to her phone. She consented and, using forensic tools, the investigator uncovered evidence indicating the woman had sought out a stranger via an Internet advertisement with the intent to get pregnant. To cover her infidelity, she fabricated the story that a stranger had raped her. When confronted with the communications recovered from her phone, the woman admitted the rape report was false. Without the digital evidence, an innocent man may well have been accused of a violent sexual assault.

Another investigation in Clark County, Nevada, centered on allegations that a woman and her boyfriend conspired together to kill the woman's father who died after being stabbed

approximately 30 times. Text messages which had been deleted from the phone and recovered by investigators revealed the couple's plans in detail, clearly showing premeditation. Additionally, the communications around the time of the killing proved that both of them were involved throughout the process and during the entire event, resulting in both being charged with murder and conspiracy to commit murder.

Following a joint investigation conducted by the FBI and Indiana State Police, a pastor pleaded guilty in Federal court to transporting a minor across state lines with intent to engage in illicit sexual conduct in connection with his sexual relationship with an underage girl who was a student at the church's high school. During this investigation, information recovered from the pastor's smart phone proved to be crucial in showing the actions taken by the pastor in the commission of his crimes. Using forensic software, investigators identified Wi-Fi locations, dates, and times when the pastor traveled out of state to be with the victim. The analysis uncovered Internet searches including, "What is the legal age of consent in Indiana", "What is the legal age of consent in Michigan", and "Penalty for sexting Indiana." In addition, image files were located which depicted him in compromising positions with the victim.

These are examples of how important evidence that resides on smart phones and other devices can be to law enforcement – evidence that might not have been available to us had strong encryption been in place on those devices and the user's consent not granted.

The above examples serve to show how critical electronic evidence has become in the course of our investigations and how timely, reliable access to it is imperative to ensuring public safety. Today's encryption methods are increasingly more sophisticated, and pose an even greater challenge to law enforcement. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop – evidence that may be the difference between an offender being convicted or acquitted – but we cannot access it.

Previously, a company that manufactured a communications device could assist law enforcement in unlocking the device. Today, however, upon receipt of a lawful court order, the company might only be able to provide information that was backed up in the cloud – and there is no guarantee such a backup exists, that the data is current, or that it would be relevant to the investigation. If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.

Civil Liberties and the Rule of Law

Just as we have an obligation to address threats to our national security and our public safety, we also have an obligation to consider the potential impact of our investigations on civil liberties, including the right to privacy.

Intelligence and technology are key tools we use to stay ahead of those who would do us harm. Yet, as we evolve and adapt our investigative techniques and our use of technology to keep pace with today's complex threat environment, we must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution.

The people of the FBI are sworn to protect both security and liberty. We care deeply about protecting liberty – including an individual's right to privacy through due process of law – while simultaneously protecting this country and safeguarding the citizens we serve.

The rule of law is our true north; it is the guiding principle for all that we do. The world around us continues to change, but within the FBI, our values must never change. Every FBI employee takes an oath promising to uphold the United States Constitution. It is not enough to catch the criminals; we must do so while upholding civil rights. It is not enough to stop the terrorists; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights are not burdens. They are what make all of us safer and stronger. In the end, we in the FBI will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

And with the rule of law as our guiding principle, we also believe that no one in this country should be beyond the law. We must follow the letter of the law, whether examining the contents of a suspected individual's closet or the contents of her smart phone. But the notion that the closet could never be opened – or that the phone could never be unlocked or unencrypted – even with a properly obtained court order, is troubling.

Are we as a society comfortable knowing that certain information is no longer available to law enforcement under any circumstances? Is there no way to reconcile personal privacy and public safety? It is time to have open and honest debates about these issues.

Where Do We Go From Here?

The FBI confronts serious threats to public safety every day. So in discussing developments that thwart the court-authorized tools we use to investigate suspected criminals, we must be sure to understand what society gains, and what we all stand to lose. What is law enforcement's recourse when we are not able to access stored data and real-time communications, despite having a court order? What happens when we cannot decipher the passcode? What happens if there are no other means to access the digital evidence we need to find a victim or prosecute a criminal? We will use every lawfully authorized investigative tool

we have to protect the citizens we serve, but having to rely on those other tools could delay criminal investigations, preclude us from identifying victims and co-conspirators, risk prematurely alerting suspects to our investigative interests, and potentially put lives in danger.

We will continue to work with our Federal, State, tribal, and local partners to identify a path forward. We are thankful for Congress' support in funding the National Domestic Communications Assistance Center, which will enable law enforcement to share tools, train one another in available intercept solutions, and reach out to the communications industry with one voice.

Companies must continue to provide strong encryption for their customers and make every effort to protect their privacy, but so too does law enforcement have a real need to obtain certain communications data when ordered by a court of law. We care about the same things – safety, security, and prosperity. And from the FBI's perspective, we know an adversarial posture won't help any of us in achieving those things. We must challenge both government and industry to develop innovative solutions to secure networks and devices, yet still yield information needed to protect our society against threats and ensure public safety.

Perhaps most importantly, we need to make sure the American public understands the issues and what is at stake.

I believe we can come to a consensus, through a reasoned and practical approach. And we must get there together. It is only by working together – within the law enforcement and intelligence communities, with the private sector, and with our elected officials – that we will find a long-term solution to this growing problem.

We in the FBI want to continue the discussion about how to solve these serious problems. We want to work with Congress, with our colleagues in the private sector, with our law enforcement and national security partners, and with the people we serve, to find the right balance for our country.

Conclusion

Chairman Hurd, Ranking Member Kelly, and members of the committee, I thank you for this opportunity to discuss the FBI's priorities and the challenges of Going Dark. The work we do would not be possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.

###