PERSONAL TECHNOLOGY ENCRYPTION VS. HOMELAND SECURITY

BY MICHAEL ERBSCHLOE

Personal Technology Encryption

Vs.

Homeland Security

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the
U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational
Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business
Privacy Plan (McGraw Hill)

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly 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.

Private Citizens care deeply about privacy, and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take 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. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked 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, and child exploitation—where critical evidence came from smart phones, computers, and online communications.

When changes in technology hinder law enforcement’s ability to exercise investigative tools and follow critical leads, 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 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 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.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, 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. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in 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.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully authorized access to their data, the jury would not have been able to consider

that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the government to conduct real-time—i.e., data in motion—electronic surveillance of the content of a suspect's communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as "Title III" or the "Wiretap Act") or the Foreign Intelligence Surveillance Act of 1978 (or "FISA"). Title III authorizes the government to obtain a court order to conduct surveillance of wire, oral, or electronic communications when it is investigating federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court (FISC), to approve surveillance directed at foreign intelligence and international terrorism threats. Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a federal district court judge must find:

That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;
That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and
That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the government seeks to extend surveillance beyond this period, it must submit another application with a fresh showing of probable cause and investigative necessity. And the government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

That the target of the surveillance is a foreign power or agent of a foreign power; and
That each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information stored—i.e., data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Source: https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

Law enforcement has concerns over certain technological changes, and there are fears that officials may be unable to keep pace with technological advances and conduct electronic surveillance if they cannot access certain information. Originally, the going dark debate centered on law enforcement's ability to

intercept real-time communications. More recent technology changes have potentially impacted law enforcement capabilities to access not only communications, but stored data as well. There are concerns that enhanced encryption may affect law enforcement investigations, though there is limited empirical evidence. If evidence arises that investigations are hampered, policy makers may question what, if any, actions they should take. One option is that Congress could update electronic surveillance laws to cover data stored on smartphones. Congress could also prohibit the encryption of data unless law enforcement could still access the encrypted data. They may also consider enhancing law enforcement's financial resources and manpower, which could involve enhancing training for existing officers or hiring more personnel with strong technology expertise.

Some of these options may involve the application of a "back door" or "golden key" that can allow for access to smartphones. However, as has been noted, "when you build a back door for the good guys, you can be assured that the bad guys will figure out how to use it as well." This is the tradeoff. Policy makers may debate which—if either—may be more advantageous for the nation on the whole: increased security coupled with potentially fewer data breaches and possibly greater impediments to law enforcement investigations, or increased access to data paired with potentially greater vulnerability to malicious actor.

Source: https://www.hsdl.org/?view&did=787160

Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?

James B. Comey
Director
Federal Bureau of Investigation

Brookings Institution
Washington, D.C.
October 16, 2014

Remarks as delivered.

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to express my tenure in terms of months, and I joke that I have eight years and 11 months to go, as if I'm incarcerated. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed—that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the core of the FBI. It is the organization's spine.

But we confront serious threats—threats that are changing every day. So I want to make sure I have every lawful tool available to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk in a serious way about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect and the capabilities we have for collecting information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support. We have no monopoly on wisdom.

My goal today isn't to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation as a country about where we are, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data—you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first, and then we'll talk about challenges posed by different means of encryption.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, countless networks, and countless means of communicating. We have laptops, smartphones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to cover up what they're doing. And that makes it tough for us to keep up.

If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time—that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the

evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks—all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

At the outset, Apple says something that is reasonable—that it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud" and that the FBI can still access that data with lawful authority. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud and to make sure that law enforcement cannot access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called "brute force" attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, "Can't you just compel the owner of the phone to produce the password?" Likely, no. And even if we could compel them as a legal matter, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for refusing to comply with a court order to produce his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or e-mail or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call this FOMO, or "fear of missing out."

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us...missing out on violent criminals who target our communities...missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case—from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation—where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages stored on her parents' cell phones to one another and to their family members proved the mother caused this young girl's death and that the father knew what was happening and failed to stop it. Text messages stored on these devices also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them—killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later. Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

These are cases in which we had access to the evidence we needed. But we're seeing more and more cases where we believe significant evidence is on that phone or a laptop, but we can't crack the password. If this becomes the norm, I would suggest to you that homicide cases could be stalled, suspects could walk free, and child exploitation might not be discovered or prosecuted. Justice may be denied, because of a locked phone or an encrypted hard drive.

My Thoughts

I'm deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do and how we do it.

I hope you know that I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government—and of law enforcement—that we are willing to let bad guys walk away...willing to leave victims in search of justice?

There will come a day—and it comes every day in this business—where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of government power. I am. This country was founded by people who were worried about government power—who knew that you cannot trust people in power. So they divided government power among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the founders intended—that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty—the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve—in every investigation.

Where Do We Go from Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life—that smart people can come to the right answer.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains and what we all stand to lose.

We in the FBI will continue to throw every lawful tool we have at this problem, but it's costly. It's inefficient. And it takes time.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common

ground. We care about the same things. I said it because I meant it. These companies are run by good people. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard and so that those of us in law enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer—to find the balance we need.

Thank you for having me here today

Source: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Chairman Goodlatte Statement at Encryption Hearing March 2, 2016

We welcome everyone today to this timely and important hearing on encryption.

Encryption is a good thing. It prevents crime, it prevents terrorist attacks. It keeps our most valuable information safe. Yet it is not used as effectively today as is necessary to protect against the ever increasing sophistication of foreign governments, criminal enterprises and just plain hackers.

We see this manifest almost every week in the reports of losses of massive amounts of our most valuable information from government agencies, retailers, financial institutions, and individuals. From identity theft to the compromising of our infrastructure, to our economic and military security, encryption must play an ever-increasing role and the companies that develop it must be encouraged to increase its effectiveness.

Encryption is a topic that may sound arcane or only the province of "techies," but, in fact, is a subject whose solutions will have far-reaching and lasting consequences.

The Judiciary Committee is a particularly appropriate forum for this Congressional debate to occur. As the committee of exclusive jurisdiction over the U.S. Constitution, the Bill of Rights, and the federal criminal laws and procedures, we are well-versed in the perennial struggle between protecting Americans' privacy and enabling robust public safety. This Committee is accustomed to addressing many of the significant legal questions arising from laws that govern surveillance and government access to communications, particularly the Wiretap Act, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, and the Communications Assistance to Law Enforcement Act, otherwise known as CALEA.

Today's hearing is a continuation of the Committee's work on encryption – work that Congress is best-suited to resolve.

As the hearing title indicates, society has been walking a tightrope for generations in attempting to balance the security and privacy of Americans' communications with the needs of our law enforcement and intelligence agencies. In fact, the entire world now faces a similar predicament, particularly as our commerce and communications bleed over international boundaries on a daily basis.

Encryption, in securing data in motion and in storage, is a valuable technological tool that enhances Americans' privacy, protects our personal safety and national security, and ensures the free flow of our nation's commerce. Nevertheless, as encryption has increasingly become a ubiquitous technique to secure communications among consumers, industry, and governments, a national debate has arisen concerning the positive and negative implications for public safety and national security.

This growing use of encryption presents new challenges for law enforcement seeking to obtain information during the course of its investigations, and even more foundationally, tests the basic framework that our nation has historically used to ensure a fair and impartial evaluation of legal process used to obtain evidence of a crime.

We must answer this question: how do we deploy ever stronger, more effective encryption without unduly preventing lawful access to communications of criminals and terrorists intent on doing us harm? This now seems like a perennial question that has challenged us for years.

In fact, over 15 years ago I led congressional efforts to ensure strong encryption technologies and to

ensure that the government could not automatically demand a backdoor key to encryption technologies. This enabled the U.S. encryption market to thrive and produce effective encryption technologies for legitimate actors rather than see the market head completely overseas to companies that do not have to comply with basic protections.

However, it is also true that this technology has been a devious tool of malefactors. Here is where our concern lies. Adoption of new communications technologies by those intending harm to the American people is outpacing law enforcement's technological capability to access those communications in legitimate criminal and national security investigations.

Following the December 2015 terrorist attack in San Bernardino, California, investigators recovered a cell phone owned by the county government but used by one of the terrorists responsible for the attack. After the FBI was unable to unlock the phone and recover its contents, a federal judge ordered Apple to provide "reasonable technical assistance to assist law enforcement agents in obtaining access to the data" on the device, citing the All Writs Act as its authority to compel.

Apple has challenged the court order, arguing that its encryption technology is necessary to protect its customers' communications' security and privacy, and raising both constitutional and statutory objections to the magistrate's order.

This particular case has some very unique factors involved and as such may not be an ideal case upon which to set precedent. And it is not the only case in which this issue is being litigated. Just yesterday, a magistrate judge in the Eastern District of New York ruled that the government cannot compel Apple to unlock an iPhone pursuant to the All Writs Act. It is clear that these cases illustrate the competing interests at play in this dynamic policy question – a question that is too complex to be left to the courts and must be answered by Congress.

Americans surely expect that their private communications are protected. Similarly, law enforcement's sworn duty is to ensure that public safety and national security are not jeopardized if possible solutions exist within their control.

This body, as well, holds its own Constitutional prerogatives and duties. Congress has a central role to ensure that technology advances so as to protect our privacy, help keep us safe, and prevent crime and terrorist attacks. Congress must also continue to find new ways to bring to justice criminals and terrorists.

We must find a way for physical security not to be at odds with information security. Law enforcement must be able to fight crime and keep us safe, and this country's innovative companies must at the same time have the opportunity to offer secure services to keep their customers safe.

The question for Americans and lawmakers is not whether or not encryption is essential, but instead, whether law enforcement should be granted access to encrypted communications when enforcing the law and pursuing their objectives to keep our citizens safe.

I look forward to hearing from our distinguished witnesses today as the Committee continues its oversight of this real-life dilemma facing real people all over the globe.

Source: https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/

Deputy Attorney General Rod J. Rosenstein Remarks on Encryption at the U.S. 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 7,500 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.

Source:
https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

Encryption and Cyber Security for Mobile Electronic Communication Devices

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

Statement Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology
Washington, D.C.
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, e-mail, text messages and chat sessions in transit. The second challenge concerns legally authorized access to data stored on devices, such as e-mail, 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 cyber security 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, e-mail, 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 cyber crime 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 not lower 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.

Source: https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices

Introduction to Encryption Export Controls

Welcome to the Department of Commerce Bureau of Industry and Security Export Regulations Training Webinar Series. Today's topic is an "Introduction to Encryption Export Controls." In just a moment we'll be turning you over to our presenters. If you're watching live you'll have the opportunity to ask questions directly using the "Ask a question" button just below the video window. We hope you enjoy the view overlooking Connecticut Avenue and K Streets in Washington, only a couple blocks from the White House. Again, thank you for attending. Now let's turn it over to our presenters.

The Information Technology Controls Division is pleased to present this brief webinar, with an introductions to Encryption Export Controls this afternoon. The Information Technology Controls Division consists of nine licensing officers; myself, Randy Wheeler, and I'm joined today by two other licensing officer, Anita Zinzuvadia and Aaron Amundson. We're going to very quickly run through a list of topics to familiarize you with the encryption export controls and the Export Administration Regulations.

The Information Technology Controls Division is responsible for classifying and licensing items that are listed in Categories 4, 5 Part 1, and 5 Part 2 of Commerce Control list; that is, computer, communications, and information security items. And we have found that at least 95% of our workload is concerned with encryption items that are found in Category 5 Part 2 of the Commerce Control list.

Before launching into our slides, I would like to make a couple of notes. One is, again, this is a very brief webinar. We're going to run through a lot of terminology very quickly. But we hope that questions that come up, you will feel free to contact us after the webinar. We'll have our contact information at the end of the presentation, and we would be happy to talk to you and answer any further questions that you have.

Secondly, we are presenting the encryption provisions of the Export Administration Regulations as they are today, February 17th, 2016, and the regulations do change from time to time. In fact, as we speak, there is a rule making its way through to publication that will make some structural changes to Category 5 Part 2 of the Commerce Control list. We also hope that some additional provisions, encryption provisions, can be amended in the same rule. So, please, if you are looking to the encryption provisions, please make sure that you look at the current version of the Export Administration Regulations that are published on our website, as things do change.

Finally, just to note that there are a few handouts that are included in the webinar materials today. We have two charts, one on license exception ENC, and one on mass market encryption, and two lists of government end-users that I will be discussing later on in the presentation. So with that, I'd like to turn the slides over to Anita Zinzuvadia. These are the topics that we're going to touch on today very briefly, and we will start with the Category 5 Part 2 of the Commerce Control List.

Thank you, Randy. So I'm going to take a few minutes to discuss items that are subject to Category 5 Part 2. And when I start these discussions I like to kind of start off with a common base of understanding. And with that, first, I'd like to talk about some items that are not in Category 5 Part 2. First of all, encrypted data: the EAR, Export Administration Regulations, does not control encrypted data for the sake of it being encrypted. So that includes files, music, multimedia information, videos. Encrypted data is not controlled. But the hardware/software that could be used to encrypt that data could be controlled. So that's point number one there. Compression: we do not consider compression

to be cryptography. There's no means for hiding information in compression, or a secret key exchange used in compression. So, some of you may be familiar with tools like WinZip. It compresses the information using certain algorithms, but the compression itself is not considered encryption. But WinZip is a tool that we know that does encryption on top of the compression. So it could be considered an encryption item for the functionality but not the compression itself.

Next, coding techniques, we outline this in the regulations under Category 5 Part 2 that we do not control fixed coding techniques. Things like CDMA is not considered cryptography. Also, parity bits are not considered with your key length in encryption in counting your -- measuring your key length.

And as I said at the beginning, there is a chart in the handout that provides another table with the different types of mass market authorization. Now we've gone through all of the different authorizations that are available for -- under license exception ENC and mass market. So that's all of the different authorizations that are available. And now I'm going to talk about once you figure out whether you need the registration, the classification, or the reporting, the mechanics of how you do that, how you submit the different forms that are required.

First is the encryption registration. And as a reminder, the encryption registration is required for all of the (b)(1), (b)(2), and (b)(3) items under both ENC and mass market. The encryption registration is a separate module in SNAPR called the "encryption registration." You fill out the encryption registration form in SNAPR and you attach the Supplement 5, the answers to the questions that are in Supplement 5 to Part 742. You attach that in SNAPR and then you submit it. And then the system will basically automatically send you back the encryption registration number, and that's it.

That's the entire process for getting the encryption registration. The encryption registration is really a company registration. It's not a product registration. So the regulations only require you to submit one registration per company. And the registration only needs to be updated once a year. That's a calendar year. Once per calendar year, and only if something changes in the registration. So the most you should ever have to submit an encryption registration is once a year, and then only if something changed in your registration from the previous year.

If you are not the manufacturer of an item you can rely on the manufacturer's encryption registration, if they have one. If you want to export a (b)(1) product and you don't have an encryption registration but the manufacturer had told you they have an encryption registration, then you can rely on the manufacturer's encryption registration. You wouldn't need to submit one of your own. That's the registration requirement.

The classification requirement, again, the classification is required for items in (b)(2) and (b)(3) of ENC, and mass market (b)(3). For the classification request, you fill out the same commodity classification request form in SNAPR and then you attach a data sheet or equivalent, something equivalent to the data sheet. And you provide the answers to the questions that are in Supplement 6, to part 742. Those are all the questions on the encryption functionality. And then you submit that. And once you submit the complete review request, so the review request with the data sheet and the Supplement 6 information, once you submit the review request, you can start exporting immediately to the Supplement 3 countries.

You don't have to wait to hear anything from us. You can export immediately to the Supplement 3 countries. Then, 30 days later, you can start exporting under the full authorization of license exception ENC, even if we haven't issued the classification yet. And the 30 days doesn't include days that we've

put the application on hold, but if you submit a classification request and 30 days go by and you haven't heard anything from us on the classification, then you can start using license exception ENC under the authorization that you requested. Once you have a completed classification request, and we've issued the classification request, a new classification is only required if you make changes to the encryption functionality of the product. So you can make other changes to the product. You can change the name of the product. You can make other changes that don't affect the encryption, and you don't need to come in for a new classification request for that. You only need to come in for a new classification request as soon as you start making changes to the encryption functionality of the product.

And the last thing that I'll talk about, then, is the reporting requirements. Now under the license exception ENC in mass market there's two types of reporting requirements. The first is the semiannual sales report, and that's required for the (b)(2) items and the (b)(3)(iii) items, the forensic and packet inspection network analysis products. Those require a semiannual sales report. You have to basically report each transaction that you made under those provisions. The reporting for the semiannual sales report is only required for exports from the U.S. and for re-exports from Canada. So re-exports from other countries don't require any reporting, only exports from the U.S. and from Canada.

There's a few exceptions to the reporting requirements also, which you can see in 740.17(e). And for this report, the semiannual sales report, there's no specific formatting requirements that are required by the regulations. As long as you provide the information that it asks for you can put it in whatever format works for you.

The other type of reporting is the annual self-classification report. And self-classification is a little bit of a misnomer. It's not really just for products that you self-classified, it's required for all (b)(1) items that you exported under your own encryption registration number. And it's not a transaction report, it's just a report that lists the products that you have been exporting under Paragraph (b)(1). And that report has specific format requirements. It has to be in a CSV format with six specific data fields. And all the details for that are in Supplement 8 to Part 742 of the EAR. And then the last thing I'll note is that, as you can see, there's no reporting required for any of the (b)(3) items except for the (b)(3)(iii) items. But the other (b)(3) items don't have any reporting requirements that are associated with them. And with that, I'll turn it over to Randy.

Thank you. We have two quick topics to cover before we start taking questions and answers. The first topic is encryption licenses and encryption licensing arrangements. Now as we've heard from Anita and Aaron, a lot of products, a lot of transactions are eligible for either decontrol under mass market or for license exception ENC. So what we're left with, for licensing purposes, are those restricted (b)(2) products that are being exported to government end users, for the most part in non-Supplement 3 countries.

We also have encryption licensing for encryption technology for the development and manufacture of encryption products abroad and, of course, there would be licensing required for exports to the embargoed countries. Those licenses, our division doesn't handle. They are handled by the foreign policy division. As a general matter, our approval rate for export licensing is very high. There are very few end users or destinations that are problematic. In fact, the licensing is more for making sure we know what is going where, as opposed to trying to control it from going there. So, generally, we have a very high approval rate for our export licensing.

Now, as we heard from Aaron, the license exception ENC authorization is generally to non-government

end users, so the licenses are required for government end users. And we do have a definition of government end user in the regulations in Section 772.1. As a general chapeau, the definition would encompass any foreign central, regional, or local government departmental agency or other entity performing governmental functions, including research institutes, and also companies that are owned by the government that manufacture products on the Wassenaar Munitions List.

Our definition of government end user does have a number of exclusions. It wouldn't be an encryption provision if it didn't have several layers. And the exclusions include utilities, including telecommunications and internet service providers; banks, financial institution; transportation entities such as government-owned airlines, or government-owned railroads, government-owned entertainment organizations; educational organizations. But this exclusion does not include research institutions or public schools and universities. And finally, the last exclusion is for civil health and medical organizations.

So none of those are considered to be government end users, and people, exporters do have problems often, with trying to determine under this definition whether a particular foreign entity would or would not be considered a government end user under the definition. We do consider it our responsibility to make that determination, so if there's a question about an entity, please feel free to e-mail us with whatever information you have, or a website, and we'll look at it and try to decide whether we would consider it a government end user or not.

If there simply isn't enough information to make the determination, we would default to determining that it is a government end user. But in many situations we can provide our written determination that an entity is not considered a government end user under this definition; therefore the transaction would be eligible for license exception ENC.

Now because we have a large quantity of export licensing for encryption products, although we do offer the normal individual validated license, which is for a specified quantity of products to a specific end user, we also have a vehicle called an "Encryption Licensing Arrangement," which is mentioned in the regulations but isn't really discussed very thoroughly, and has sort of grown up on its own as a practical matter as opposed to a regulatory vehicle. An Encryption Licensing Arrangement is available for unlimited quantities of products, may include a long list of products, and may be for a range of end users as well.

Generally speaking, the Encryption Licensing Arrangements are for a four-year validity period, and over time we have developed two different kinds of encryption licensing arrangements. We've divided government end users into two different lists, less sensitive and more sensitive. For the less sensitive government end users we offer what we refer to as "Worldwide ELAs." They do not include authorization to the embargoed countries but to all other destinations. And this is one license that we issue for all of these destinations. The licenses, as issued, have various end users and in various countries. That's how the license reads. And for those Encryption Licensing Arrangements, the condition is usually a semiannual sales report, which is, as we know, very similar to what is available for non-government end users for (b)(2) products under license exception ENC. So the difference between a worldwide Encryption Licensing Arrangement
and licensing exception ENC authorization is very small.

We also have a list of more sensitive government end users. And to date, we've only been able to issue these for one country at a time. So we also refer to these as "Single-country ELAs." The condition on

these authorizations is generally a 15-day pre-shipment notification. The notification is submitted by e-mail to both BIS and to NSA, and it doesn't mean that we all come back and say, "No, you can't ship the product." The notification is also there. It's simply a notification to say we're sending this product to this end user in this country.

So the two handouts that -- two of the handouts that were included with the materials include these lists of less sensitive and more sensitive government end users. And, to date, we have been able to place any government end user that we have run across in one of these lists. There may be a time when I can't say that, but, to date, we've been able to find a paragraph to put every government end user that we have identified. And we encourage the use of the ELAs, both to save time for exporters and to save time for us with processing license applications.

The last topic that I'll touch on for purposes of this webinar is publicly available encryption software. Anita mentioned publicly available encryption items as not being subject to the Category 5 Part 2 controls. In fact, we do retain jurisdiction for encryption source code. It does remain classified under ECCN 5D002, even if it is publicly available. And the statement of this retention of jurisdiction is set forth in Section 734.3 of the regulations.

This does not apply to publicly available encryption technology. Technology can be made available and published, and it is not subject to the EAR. But source code is, to date, still subject. However, it is not restricted and can be exported under licensing exception TSU, or Technology and Software Unrestricted, after a notification is submitted by e-mail to BIS and to the National Security Agency. That notification states where the source code is posted on the Internet, or the notification can be a copy of the source code that's posted.

Object code that's compiled from source code and made eligible for license exception TSU, and that also meets the publicly available criteria set forth in Section 734 becomes not subject to the regulations. And publicly available mass market encryption software is no longer subject to the EAR. But I included this slide because in order for a mass market encryption software to be publicly available and not subject to the EAR, the process for making it mass market to begin with has to be followed. So the process is to submit an encryption registration and to self classify the mass market software, and then to make it publicly available so it is no longer subject to the regulation.

Source: https://bis.doc.gov/index.php/documents/pdfs/1441-encryption-webinar-transcript-2861771-introduction-to-encryption-export-controls/file

Encryption items NOT Subject to the EAR

There are no EAR obligations associated with the item unless it is exported, reexported, or transferred. These are specially defined terms in the EAR. See Section 734 for guidance on the definition of export, reexport, and transfer.
Certain foreign made items that contain less than a de minimis amount of U.S. origin content are not subject to the EAR. See 734.4 of the EAR.

Publicly Available:
Encryption items that are publicly available as further described below are not subject to the Export Administration Regulation. Sections 734.3(b)(3) and 734.7 define what is publicly available and published. Common examples are free apps posted online or mass market software available as a free download.

Specifically:
1. Mass market encryption object code software that is made "publicly available"

•Once the mass market item is properly classified under the relevant section of 740.17(b)(1) or (b)(3) (after a classification by BIS (5D992.c) or self-classification with self-classification report), if the software is then made "publicly available" it is not subject to the EAR.

•For example, an App made for a smartphone or computer that that meets the Mass Market criteria (as described in Note 3 of Cat. 5 Part 2) that is made available free of charge would be considered "publicly available". In this case you would have to first comply with the mass market requirement under 740.17 (b)(1) or (b)(3) by self-classification as 5D992.c with self-classification report (or submitting classification request to BIS) only once. Then, if the item is made publicly available (e.g., free to download) it would be considered not subject to the EAR anymore.

"Publicly available" encryption source code is not subject to the EAR once the email notification per section 742.15(b) is sent.

•A common example would be open source encryption source code available for free online.

"Publicly available" encryption object code is not subject to the EAR when the corresponding source code is also "publicly available" and has been notified as specified under Part 742.15(b).
Note 1: Notifications made before September 2016 under License Exception TSU (740.13) remain valid under 742.15. A new notification is not required.
Note 2: While open source code itself may be publicly available and not subject to the EAR, an item is not considered publicly available merely because it incorporates or calls to publicly available open source code. Rather, a new item with encryption functionality has been created which would need to be evaluated as a whole under the EAR.

Source: bis.doc.gov/index.php/policy-guidance/encryption/1-encryption-items-not-subject-to-the-ear

Title 15: Commerce and Foreign Trade
PART 740—LICENSE EXCEPTIONS
§740.17 Encryption commodities, software, and technology (ENC).

License Exception ENC authorizes export, reexport, and transfer (in-country) of systems, equipment, commodities, and components therefor that are classified under ECCNs 5A002, 5B002, equivalent or related software and technology therefor classified under 5D002 or 5E002, and “cryptanalytic items” classified under ECCNs 5A004, 5D002 or 5E002. This License Exception ENC does not authorize export or reexport to, transfer (in-country) in, or provision of any service in any country listed in Country Groups E:1 or E:2 in supplement no. 1 to part 740 of the EAR, or release of source code or technology to any national of a country listed in Country Groups E:1 or E:2. Reexports and transfers (in-country) under License Exception ENC are subject to the criteria set forth in paragraph (c) of this section. Paragraphs (b) and (d) of this section set forth information about classifications required by this section. Items described in paragraphs (b)(1) and (b)(3)(i), (ii), or (iv) of this section that meet the criteria set forth in Note 3 to Category 5—Part 2 of the Commerce Control List (the “mass market” note) are classified under ECCN 5A992.c or 5D992.c following self-classification or classification by BIS and are no longer subject to “EI” and “NS” controls. Paragraph (e) sets forth reporting required by this section. For items exported under paragraphs (b)(1), (b)(3)(i), (ii), or (iv) of this section and therefore excluded from paragraph (e) reporting requirements, exporters are reminded of the recordkeeping requirements in part 762 of the EAR and that they may be required to make such records available upon request. All classification requests, and reports submitted to BIS pursuant to this section for encryption items will be reviewed by the ENC Encryption Request Coordinator, Ft. Meade, MD.

(a) No classification request or reporting required. License Exception ENC authorizes the export, reexport, or transfer (in-country) to the end users and for the end uses set forth in paragraphs (a)(1) through (3) of this section, without submission of a classification request, self-classification report or sales report to BIS.

(1) Certain exports, reexports, transfers (in-country) to 'private sector end users'—(i) Internal “development” or “production” of new products. License Exception ENC authorizes certain exports, reexports, and transfers (in-country) of items described in paragraph (a) of this section for the internal “development” or “production” of new products by 'private sector end users,' wherever located, that are headquartered in a country listed in supplement no. 3 of this part.

(ii) Certain exports, reexports, transfers (in-country) to related parties, not involving “development” or “production” of new products. For internal end uses among 'private sector end users' other than the “development” or “production” of new products, License Exception ENC authorizes exports, reexports, and transfers (in-country) of non-U.S.-origin items, described in paragraph (a) of this section, to 'private sector end users' wherever located provided that:

(A) That item became subject to the EAR after it was produced;

(B) All parties to the transaction are subsidiaries of the same parent company headquartered in a country listed in supplement no. 3 of this part; and

(C) The characteristics or capabilities of the existing item are not enhanced, unless otherwise authorized by license or license exception.

Note to paragraph (a)(1): A 'private sector end user' is either: An individual who is not acting on behalf

of any foreign government; or a commercial firm (including its subsidiary and parent firms, and other subsidiaries of the same parent) that is not wholly owned by, otherwise controlled by or acting on behalf of, any foreign government.

(2) Exports, reexports, transfers (in-country) to "U.S. Subsidiaries." License Exception ENC authorizes export, reexport, and transfer (in-country) of items described in paragraph (a) of this section to any "U.S. subsidiary," wherever located. License Exception ENC also authorizes export, reexport, transfer (in-country) of such items by a U.S. company and its subsidiaries to foreign nationals who are employees, individual contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use, including the "development" or "production" of new products, without prior review by the U.S. Government.

Note to paragraphs (a)(1) and (2): All items produced or developed with items exported, reexported, or transferred (in-country) under paragraphs (a)(1) or (2) of this section are subject to the EAR. These items may require the submission of a classification request before sale, reexport or transfer to non-"U.S. subsidiaries," unless otherwise authorized by license or license exception.

(3) Reexports and transfers (in-country) of non-U.S. products developed with or incorporating U.S.-origin encryption source code, components, or toolkits. License Exception ENC authorizes the reexport and transfer (in-country) of non-U.S. products developed with or incorporating U.S.-origin encryption source code, components or toolkits that are subject to the EAR, provided that the U.S.-origin encryption items have previously been classified or reported and authorized by BIS and the cryptographic functionality has not been changed. Such products include non-U.S. developed products that are designed to operate with U.S. products through a cryptographic interface.

Note to paragraph (a)(3): This exception from classification and reporting requirements does not apply to non-U.S.-origin products exported from the United States.

(b) Classification request or self-classification report. For products described in paragraph (b)(1) of this section that are self-classified by the exporter, a self-classification report in accordance with paragraph (e)(3) of this section is required from specified exporters, reexporters and transferors; for products described in paragraph (b)(1) of this section that are classified by BIS via a CCATS, a self-classification report is not required. For products described in paragraphs (b)(2) and (3) of this section, a thirty-day (30-day) classification request is required in accordance with paragraph (d) of this section. An exporter, reexporter, or transferor may rely on the producer's self-classification (for products described in (b)(1), only) or CCATS for an encryption item eligible for export or reexport under License Exception ENC under paragraph (b)(1), (2), or (3) of this section. Exporters are still required to comply with semi-annual sales reporting requirements under paragraph (e)(1) or (2) of this section, even if relying on a CCATS issued to a producer for specified encryption items described in paragraphs (b)(2) and (b)(3)(iii) of this section.

Note to paragraph (b) introductory text: Mass market encryption software that would be considered publicly available under §734.3(b)(3) of the EAR, and is authorized for export under this paragraph (b), remains subject to the EAR until all applicable classification or self-classification requirements set forth in this section are fulfilled.

(1) Immediate authorization. This paragraph (b)(1) authorizes the exports, reexports, and transfers (in-country) of the associated commodities self-classified under ECCNs 5A002.a or 5B002, and equivalent or related software therefor classified under 5D002, except any such commodities, software, or

components described in (b)(2) or (3) of this section, subject to submission of a self-classification report in accordance with §740.17(e)(3) of the EAR. Items described in this paragraph (b)(1) that meet the criteria set forth in Note 3 to Category 5—Part 2 of the Commerce Control List (the “mass market” note) are classified as ECCN 5A992.c or 5D992.c following self-classification or classification by BIS and are removed from “EI” and “NS” controls.

(2) Classification request required. Thirty (30) days after the submission of a classification request with BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph under License Exception ENC authorizes certain exports, reexports, and transfers (in-country) of the items specified in paragraph (b)(2) and submitted for classification.

Note to paragraph (b)(2) introductory text: Immediately after the classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph also authorizes exports, reexports, and transfers (in-country) of:

1. All submitted encryption items described in this paragraph (b)(2), except “cryptanalytic items,” to any end user located or headquartered in a country listed in supplement no. 3 to this part;

2. Encryption source code as described in paragraph (b)(2)(i)(B) to non-“government end users” in any country;

3. “Cryptanalytic items” to non-“government end users,” only, located or headquartered in a country listed in supplement no. 3 to this part; and

4. Items described in paragraphs (b)(2)(iii) and (b)(2)(iv)(A) of this section, to specified destinations and end users.

(i) Cryptographic commodities, software, and components. License Exception ENC authorizes exports, reexports, and transfers (in-country) of the items in paragraph (b)(2)(i)(A) of this section to “less sensitive government end users” and non- “government end users” located or headquartered in a country not listed in supplement no. 3 to this part, and the items in paragraphs (b)(2)(i)(B) through (H) to non “government end users” located or headquartered in a country not listed in supplement no. 3.

(A) 'Network Infrastructure.' 'Network infrastructure' commodities and software, and components therefor, meeting any of the following with key lengths exceeding 80-bits for symmetric algorithms:

(1) WAN, MAN, VPN, backhaul and long-haul. Aggregate encrypted WAN, MAN, VPN, backhaul or long-haul throughput (including communications through wireless network elements such as gateways, mobile switches, and controllers) equal to or greater than 250 Mbps;

(2) [Reserved]

(3) Satellite infrastructure. Transmission over satellite at data rates exceeding 10 Mbps;

(4) Media gateways and other unified communications (UC) infrastructure, including Voice-over-Internet Protocol (VoIP) services. Media (voice/video/data) encryption or encrypted signaling to more than 2,500 endpoints, including centralized key management therefor; or

(5) Terrestrial wireless infrastructure. Air interface coverage (e.g., through base stations, access points to mesh networks, and bridges) exceeding 1,000 meters, where any of the following applies:

(i) Maximum transmission data rates exceeding 10 Mbps (at operating ranges beyond 1,000 meters); or

(ii) Maximum number of concurrent full-duplex voice channels exceeding 30;

Notes to paragraph (b)(2)(i)(A):

1. The License Exception ENC eligibility restrictions of paragraphs (b)(2)(i)(A)(3) (satellite infrastructure) and (b)(2)(i)(A)(5) (terrestrial wireless infrastructure) do not apply to satellite terminals or modems meeting all of the following:

a. The encryption of data over satellite is exclusively from the user terminal to the gateway earth station, and limited to the air interface; and

b. The items meet the requirements of the Cryptography Note (Note 3) in Category 5—Part 2 of the Commerce Control List.

2. 'Network infrastructure' (as applied to encryption items). A 'network infrastructure' commodity or software is any “end item,” commodity or “software” for providing one or more of the following types of communications:”

(a) Wide Area Network (WAN);

(b) Metropolitan Area Network (MAN);

(c) Virtual Private Network (VPN);

(d) Satellite;

(e) Digital packet telephony/media (voice, video, data) over Internet protocol;

(f) Cellular; or

(g) Trunked.

Note 1 to paragraph 2: 'Network infrastructure' end items are typically operated by, or for, one or more of the following types of end users:

(1) Medium- or large- sized businesses or enterprises;

(2) Governments;

(3) Telecommunications service providers; or

(4) Internet service providers.

Note 2 to paragraph 2: Commodities, software, and components for the “cryptographic activation” of a 'network infrastructure' item are also considered 'network infrastructure' items.

(B) Certain “encryption source code.” “Encryption source code” that is not publicly available as that

term is used in §742.15(b) of the EAR;

(C) Customized items. Encryption software, commodities and components therefor, where any of the following applies:

(1) Customized for government end users or end uses. The item has been designed, modified, adapted, or customized for "government end user(s);" or

(2) Custom or changeable cryptography. The cryptographic functionality of the item has been designed or modified to customer specification or can be easily changed by the user;

(D) Quantum cryptography. ECCN 5A002.c or 5D002 "quantum cryptography" commodities or software;

(E) [Reserved]

(F) Network penetration tools. Encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks;

(G) Public safety/first responder radio (private mobile radio (PMR)). Public safety/first responder radio (e.g., implementing Terrestrial Trunked Radio (TETRA) and/or Association of Public-Safety Communications Officials International (APCO) Project 25 (P25) standards);

(H) Specified cryptographic ultra-wideband and "spread spectrum" items. Encryption commodities and components therefor, classified under ECCNs 5A002.d or .e, and equivalent or related software therefor classified under ECCN 5D002.

(ii) Cryptanalytic commodities and software. "Cryptanalytic items" classified in ECCN 5A004 or 5D002 to non- "government end users" located or headquartered in countries not listed in supplement no. 3 to this part.

(iii) "Open cryptographic interface" items. Items that provide an "open cryptographic interface," to any end user located or headquartered in a country listed in supplement no. 3 to this part.

(iv) Specific encryption technology. Specific encryption technology as follows:

(A) Technology for "non-standard cryptography." Encryption technology classified under ECCN 5E002 for "non-standard cryptography," to any end user located or headquartered in a country listed in supplement no. 3 to this part;

(B) Other technology. Encryption technology classified under ECCN 5E002 except technology for "cryptanalytic items," "non-standard cryptography" or any "open cryptographic interface," to any non-"government end user" located in a country not listed in Country Group D:1, E:1, or E:2 of supplement no. 1 to part 740 of the EAR.

Note to paragraph (b)(2): Commodities, components, and software classified under ECCNs 5A002.b or 5D002.d, for the "cryptographic activation" of commodities or software specified by this paragraph (b)(2) are also controlled under this paragraph (b)(2).

(3) Classification request required for specified commodities, software, and components. Thirty (30)

days after a classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph authorizes exports, reexports, and transfers (in-country) of the items submitted for classification, as further described in this paragraph (b)(3), to any end user, provided the item does not perform the functions, or otherwise meet the specifications, of any item described in paragraph (b)(2) of this section. Items described in paragraphs (b)(3)(i), (ii), or (iv) of this section that meet the criteria set forth in Note 3 to Category 5—Part 2 of the Commerce Control List (the "mass market" note) are classified under ECCN 5A992.c or 5D992.c following classification by BIS.

Note to introductory text of paragraph (b)(3): Immediately after the classification request is submitted to BIS in accordance with paragraph (d) of this section and subject to the reporting requirements in paragraph (e) of this section, this paragraph also authorizes exports, reexports, transfers (in-country) of the items described in this paragraph (b)(3) to any end user located or headquartered in a country listed in supplement no. 3 to this part.

(i) "Components," toolsets, and toolkits. Specified components classified under ECCN 5A002.a and equivalent or related software classified under ECCN 5D002 not described by paragraph (b)(2) of this section, as follows:

(A) Chips, chipsets, electronic assemblies and field programmable logic devices;

(B) Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs).

(ii) "Non-standard cryptography" (by items not otherwise described in paragraph (b)(2) of this section.) Encryption commodities, software and components not described by paragraph (b)(2) of this section, that provide or perform "non-standard cryptography" as defined in part 772 of the EAR.

(iii) Advanced network vulnerability analysis and digital forensics. Encryption commodities and software not described by paragraph (b)(2) of this section, that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by any of the following:

(A) Automated network vulnerability analysis and response. Automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment; or

(B) Digital forensics, including network or computer forensics. Investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data for law enforcement purposes or in a similarly rigorous evidentiary manner.

(iv) "Cryptographic activation" commodities, components, and software. Commodities, components, and software classified under ECCNs 5A002.b or 5D002.d where the product or cryptographic functionality is not otherwise described in paragraphs (b)(2) or (b)(3)(i) of this section.

(c) Reexport and transfer (in-country). Distributors, resellers or other entities who are not original manufacturers of encryption commodities and software are permitted to use License Exception ENC only in instances where the reexport or transfer (in-country) meets the applicable terms and conditions of this section. Transfers of encryption items listed in paragraph (b)(2) of this section to "government end users," or for government end uses, within the same country are prohibited, unless otherwise

authorized by license or license exception.

(d) Classification request procedures—(1) Submission requirements and instructions. To submit a classification request to BIS, you must submit an application to BIS in accordance with the procedures described in §§748.1 and 748.3 of the EAR and the instructions in paragraph (r) of supplement no. 2 to part 748 “Unique Application and Submission Requirements,” along with other required information as follows:

(i) [Reserved]

(ii) Technical information submission requirements. For all submissions of encryption classification requests for items described under paragraph (b)(2) or (b)(3) of this section, you must submit the applicable information described in paragraphs (a) through (d) of supplement no. 6 to part 742 of the EAR (Technical Questionnaire for Encryption Items). For items eligible for self-classification that are submitted to BIS for classification you may be required to provide BIS this supplement no. 6 to part 742 information on an as-needed basis, upon request by BIS.

(iii) Changes in encryption functionality following a previous classification. A new product encryption classification request (under paragraphs (b)(2) or (b)(3) of this section) is required if a change is made to the cryptographic functionality (e.g., algorithms) or other technical characteristics affecting License Exception ENC eligibility (e.g., encrypted throughput) of the originally classified product. However, a new product classification request is not required when a change involves: the subsequent bundling, patches, upgrades or releases of a product; name changes; or changes to a previously reviewed encryption product where the change is limited to updates of encryption software components where the product is otherwise unchanged.

(2) Action by BIS.

(i) [Reserved]

(ii) For items requiring classification by BIS under paragraphs (b)(2) and (3) of this section. (A) For classifications that require a thirty (30-day) waiting period, if BIS has not, within thirty days (30 days) from registration in SNAP-R of your complete classification request, informed you that your item is not authorized for License Exception ENC, you may export, reexport, or transfer (in-country) under the applicable provisions of License Exception ENC.

(B) Upon completion of its classification, BIS will issue a Commodity Classification Automated Tracking System (CCATS) to you.

(C) Hold Without Action (HWA) for classification requests. BIS may hold your classification request without action if necessary to obtain additional information or for any other reason necessary to ensure an accurate classification. Time on such “hold without action” status shall not be counted towards fulfilling the thirty-day (30-day) processing period specified in this paragraph.

(iii) BIS may require you to supply additional relevant technical information about your encryption item(s) or information that pertains to their eligibility for License Exception ENC at any time, before or after the expiration of the thirty-day (30-day) processing period specified in this paragraph and in paragraphs (b)(2) and (3) of this section. If you do not supply such information within 14 days after receiving a request for it from BIS, BIS may return your classification request(s) without action or

otherwise suspend or revoke your eligibility to use License Exception ENC for that item(s). At your request, BIS may grant you up to an additional 14 days to provide the requested information. Any request for such an additional number of days must be made prior to the date by which the information was otherwise due to be provided to BIS, and may be approved if BIS concludes that additional time is necessary.

(e) Reporting requirements—(1) Semiannual reporting requirement. Semiannual reporting is required for exports to all destinations other than Canada, and for reexports from Canada for items described under paragraphs (b)(2) and (b)(3)(iii) of this section. Certain encryption items and transactions are excluded from this reporting requirement, see paragraph (e)(1)(iii) of this section. For information about what must be included in the report and submission requirements, see paragraphs (e)(1)(i) and (ii) of this section respectively.

(i) Information required. Exporters must include for each item, the Commodity Classification Automated Tracking System (CCATS) number and the name of the item(s) exported (or reexported from Canada), and the following information in their reports:

(A) Distributors or resellers. For items exported (or reexported from Canada) to a distributor or other reseller, including subsidiaries of U.S. firms, the name and address of the distributor or reseller, the item and the quantity exported or reexported and, if collected by the exporter as part of the distribution process, the end user's name and address;

(B) Direct sales. For items exported (or reexported from Canada) through direct sale, the name and address of the recipient, the item, and the quantity exported; or

(C) Foreign manufacturers and products that use encryption items. For exports (i.e., from the United States) or direct transfers (e.g., by a “U.S. subsidiary” located outside the United States) of encryption components, source code, general purpose toolkits, equipment controlled under ECCN 5B002, technology, or items that provide an “open cryptographic interface,” to a foreign developer or manufacturer headquartered in a country not listed in supplement no. 3 to this part when intended for use in foreign products developed for commercial sale, the names and addresses of the manufacturers using these encryption items and, if known, when the product is made available for commercial sale, a non-proprietary technical description of the foreign products for which these encryption items are being used (e.g., brochures, other documentation, descriptions or other identifiers of the final foreign product; the algorithm and key lengths used; general programming interfaces to the product, if known; any standards or protocols that the foreign product adheres to; and source code, if available).

(ii) Submission requirements. For exports occurring between January 1 and June 30, a report is due no later than August 1 of that year. For exports occurring between July 1 and December 31, a report is due no later than February 1 the following year. These reports must be provided in electronic form. Recommended file formats for electronic submission include spreadsheets, tabular text or structured text. Exporters may request other reporting arrangements with BIS to better reflect their business models. Reports may be sent electronically to BIS at crypt@bis.doc.gov and to the ENC Encryption Request Coordinator at enc@nsa.gov, or disks and CDs containing the reports may be sent to the following addresses:

(A) Department of Commerce, Bureau of Industry and Security, Office of National Security and Technology Transfer Controls, 14th Street and Pennsylvania Ave. NW., Room 2705, Washington, DC 20230, Attn: Encryption Reports, and

(B) Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Ft. Meade, MD 20755-6000.

(iii) Exclusions from reporting requirement. Reporting is not required for the following items and transactions:

(A) [Reserved]

(B) Encryption commodities or software with a symmetric key length not exceeding 64 bits;

(C) Encryption items exported (or reexported from Canada) via free and anonymous download;

(D) Encryption items from or to a U.S. bank, financial institution or its subsidiaries, affiliates, customers or contractors for banking or financial operations;

(E) [Reserved]

(F) Foreign products developed by bundling or compiling of source code.

(2) Key length increases. Reporting is required for commodities and software that, after having been classified and authorized for License Exception ENC in accordance with paragraphs (b)(2) or (3) of this section, are modified only to upgrade the key length used for confidentiality or key exchange algorithms. Such items may be exported, reexported or transferred (in-country) under the previously authorized provision of License Exception ENC without a classification resubmission.

(i) Information required. (A) A certification that no change to the encryption functionality has been made other than to upgrade the key length for confidentiality or key exchange algorithms.

(B) The original Commodity Classification Automated Tracking System (CCATS) authorization number issued by BIS and the date of issuance.

(C) The new key length.

(ii) Submission requirements. (A) The report must be received by BIS and the ENC Encryption Request Coordinator before the export, reexport or transfer (in-country) of the upgraded product; and

(B) The report must be emailed to crypt@bis.doc.gov and enc@nsa.gov.

(3) Self-classification reporting for certain encryption commodities, software and components. This paragraph (e)(3) sets forth requirements for self-classification reporting to BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD) of encryption commodities, software and components exported or reexported. This reporting requirement applies to commodities and software that meet the criteria of Note 3 to Category 5—Part 2 of the Commerce Control List (“mass market” note) and are classified under ECCN 5A992.c or 5D992.c following self-classification, as well as to commodities and software that remain classified in ECCNs 5A002, 5B002 or 5D002 following self-classification.

(i) When to report. Your self-classification report for applicable encryption commodities, software and components exported or reexported during a calendar year (January 1 through December 31) must be received by BIS and the ENC Encryption Request Coordinator no later than February 1 the following year.

(ii) How to report. Encryption self-classification reports must be sent to BIS and the ENC Encryption Request Coordinator via email or regular mail. In your submission, specify the timeframe that your report spans and identify points of contact to whom questions or other inquiries pertaining to the report should be directed. Follow these instructions for your submissions:

(A) Submissions via email. Submit your encryption self-classification report electronically to BIS at crypt-supp8@bis.doc.gov and to the ENC Encryption Request Coordinator at enc@nsa.gov, as an attachment to an email. Identify your email with subject “self-classification report.”

(B) Submissions on disks and CDs. The self-classification report may be sent to the following addresses, in lieu of email:

(1) Department of Commerce, Bureau of Industry and Security, Office of National Security and Technology Transfer Controls, 14th Street and Pennsylvania Ave. NW., Room 2099B, Washington, DC 20230, Attn: Encryption Reports, and

(2) Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Ft. Meade, MD 20755-6000.

(iii) Information to report. Your encryption self-classification report must include the information described in paragraph (a) of supplement no. 8 to part 742 for each applicable encryption commodity, software and component made eligible for export or reexport under §740.17(b)(1) of the EAR. Each product must be included in a report only one time. However, if no new products are made eligible for export or reexport during a calendar year, you must send an email to the addresses listed in paragraph (e)(3)(ii)(A) of this section stating that nothing has changed since the previous report.

(iv) File format requirements. The information described in paragraph (a) of supplement no. 8 to part 742 must be provided to BIS and the ENC Encryption Request Coordinator in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv) adhering to the specifications set forth in paragraph (b) of supplement no. 8 to part 742.

Title 15: Commerce and Foreign Trade
PART 742—CONTROL POLICY—CCL BASED CONTROLS
§742.15 Encryption items.

Encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm U.S. national security, foreign policy and law enforcement interests. The United States has a critical interest in ensuring that important and sensitive information of the public and private sector is protected. Consistent with our international obligations as a member of the Wassenaar Arrangement, the United States has a responsibility to maintain control over the export and reexport of encryption items. As the President indicated in Executive Order 13026 and in his Memorandum of November 15, 1996, exports and reexports of encryption software, like exports and reexports of encryption hardware, are controlled because of this functional capacity to encrypt information, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export or reexport may convey to others abroad. For this reason, export controls on encryption software are distinguished from controls on other software regulated under the EAR.

(a) Licensing requirements and policy—(1) Licensing requirements. A license is required to export or reexport encryption items ("EI") classified under ECCN 5A002, 5A004, 5D002.a, .c.1 or .d (for equipment and "software" in ECCNs 5A002 or 5A004, 5D002.c.1); or 5E002 for "technology" for the "development," "production," or "use" of commodities or "software" controlled for EI reasons in ECCNs 5A002, 5A004 or 5D002, and "technology" classified under 5E002.b to all destinations, except Canada. Refer to part 740 of the EAR, for license exceptions that apply to certain encryption items, and to §772.1 of the EAR for definitions of encryption items and terms. Most encryption items may be exported under the provisions of License Exception ENC set forth in §740.17 of the EAR. Following classification or self-classification, items that meet the criteria of Note 3 to Category 5—Part 2 of the Commerce Control List (the "mass market" note), are classified ECCN 5A992.c or 5D992.c and are no longer subject to this Section (see §740.17 of the EAR). Before submitting a license application, please review License Exception ENC to determine whether this license exception is available for your item or transaction. For exports, reexports, or transfers (in-country) of encryption items that are not eligible for a license exception, you must submit an application to obtain authorization under a license or an Encryption Licensing Arrangement.

(2) Licensing policy. Applications will be reviewed on a case-by-case basis by BIS, in conjunction with other agencies, to determine whether the export, reexport, or transfer (in-country) is consistent with U.S. national security and foreign policy interests. Encryption Licensing Arrangements (ELAs) may be authorized for exports, reexports, or transfers (in-country) of unlimited quantities of encryption commodities and software described in §740.17 (b)(2)(i)(A) that have been classified by BIS to "more sensitive government end users," in all destinations, except countries listed in Country Groups E:1 or E:2 of supplement no. 1 to part 740. ELAs for "more sensitive government end users" may be authorized for encryption commodities and software described in §740.17(b)(2)(ii) through (iv) under certain circumstances. ELAs are valid for four years and may require pre-shipment notification. Applicants seeking authorization for Encryption Licensing Arrangements must specify the sales territory on their license applications.

(b) Publicly available encryption source code—(1) Scope and eligibility. Subject to the notification requirements of paragraph (b)(2) of this section, publicly available (see §734.3(b)(3) of the EAR) encryption source code classified under ECCN 5D002 is not subject to the EAR. Such source code is publicly available even if it is subject to an express agreement for the payment of a licensing fee or

royalty for commercial production or sale of any product developed using the source code.

(2) Notification requirement. You must notify BIS and the ENC Encryption Request Coordinator via email of the Internet location (e.g., URL or Internet address) of the publicly available encryption source code classified under ECCN 5D002 or provide each of them a copy of the publicly available encryption source code. If you update or modify the source code, you must also provide additional copies to each of them each time the cryptographic functionality of the source code is updated or modified. In addition, if you posted the source code on the Internet, you must notify BIS and the ENC Encryption Request Coordinator each time the Internet location is changed, but you are not required to notify them of updates or modifications made to the encryption source code at the previously notified location. In all instances, submit the notification or copy to crypt@bis.doc.gov and to enc@nsa.gov.