Written Testimony
U.S. House Committee on Energy & Commerce
Subcommittee on Oversight and Investigations
Amit Yoran
President, RSA, The Security Division of EMC
April 19, 2016

Introduction

Chairman Murphy, Ranking Member DeGette, and Members of the Committee, thank you for the opportunity to testify today on encryption. This is a very complex and nuanced issue and I applaud the Committee's efforts to better understand all aspects of the debate.

My name is Amit Yoran and I am the President of RSA, The Security Division of EMC. I have spent over twenty years in the cyber security field. I received a Master of Science in computer science from the George Washington University and Bachelor of Science degree in computer science from the United States Military Academy. I served as the national cyber czar from 2003-2004 and as the founding Director of the US-CERT program. I served on the CSIS Commission on Cyber Security advising the 44th Presidency and am serving on the current Commission developing advice for the next Administration. As an innovator and entrepreneur in the security space, I founded, led and sold two major security companies: Riptech, acquired by Symantec; and NetWitness, acquired by RSA. I also serve as a director and advisor to security startups and sit on several industry advisory boards.

In my current role as President of RSA, I strive to ensure that we provide industry leading cyber security solutions for organizations worldwide.

RSA has been a cyber industry leader for more than 30 years. Our legacy is rooted in tirelessly helping customers solve their most challenging and pressing security problems. The more than 30,000 global customers we serve represent every sector of the economy. Our business enables those we work with to effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately reduce IP theft, fraud, and cybercrime. With a world-class incident response team with expertise, battle-tested processes and sophisticated tools, we have helped hundreds of customers investigate and respond to security incidents and, more importantly, recover from advanced attacks. On a broader scale, we also regularly and rapidly disseminate threat intelligence to our customers in order to empower them to take appropriate measures to protect their company assets from the ever-changing landscape of advanced threats.

Fundamental to RSA's understanding of the issues at hand is our rich heritage in encryption, which is the basis of all security technology, and reflected in our name. RSA solutions work to protect almost every industry and many nations. Our products are found in government agencies, banks, utilities, retailers, as well as hospitals and schools. At our core, we at RSA believe in the power of digital technology to fundamentally transform business and society for the better, and that the pervasiveness of our technology helps to protect everyone.

Industry and Law Enforcement Cooperation

We deeply appreciate the work of law enforcement and the national security community to protect our nation. I commend the men and women of law enforcement who have dedicated their lives to serving justice. My heartfelt sympathy goes to the families and victims of the San Bernardino attacks and the victims of other unspeakable terrorist and criminal acts.

Private industry has long partnered with law enforcement agencies to advance and protect our nation and the rule of law. Where lawful court orders mandate it or where moral alignment encourages it, many technology companies have a regular, ongoing and cooperative relationship with law enforcement in the U.S. and abroad. Simply put, it is in all of our best interests for our laws to be enforced.

A growing number of companies are publishing Transparency Reports that show the number of national security and law enforcement requests they receive and the frequency with which the companies provide the data[1]. The data shows tremendous cooperation between industry and law enforcement. Transparency Reports from six companies show they received over 88,000 requests over a one-year period and complied with over 70,000 of them, for a compliance rate of 80 percent.

"Security versus Privacy" Misnomer

The security versus privacy label is sensationalist and emotion provoking. It makes for great headlines, and acts as a looming battle-cry to rally people around the thought that we are all at grave risk if we don't empower our national security apparatus in a way that conflicts directly with our privacy. "Security versus privacy" is an incredibly inaccurate, misleading and dangerous way to describe the debate our society faces over encryption.

Today's debate needs to balance the equities of, on the one hand, the needs of law enforcement to prosecute crimes, sometimes heinous crimes, and, on the other hand, our security, privacy, and economic competitiveness. We do not face an either/or choice between security and privacy. There is a continuum of options that have to be carefully weighed as we consider the thin line that connects these issues.

To be clear, when used properly and in isolated and well-protected systems, strong encryption does make it difficult for law enforcement to access content. Encryption poses a similar challenge to our national security and intelligence community. But it also poses the same challenge to every foreign intelligence service, terrorist, criminal, hacker, industrial spy, and other bad actor attempting to affect our national security, public safety and individual rights. Strong cryptography is a foundational building block for good cybersecurity. We would simply cease to function as a technology-enabled society without it.

[1] Access Now, "Transparency Reporting Index", https://www.accessnow.org/transparency-reporting-index/, (Feb 18, 2016)

Going Dark

We live in a "golden age" of surveillance, more so than in any other point in history. In just about everything we do, we leave an incredibly insightful digital breadcrumb trail. As technologies permeate every aspect of our daily lives, this trail has exploded in a robust and detailed journaling of our activities and communications. Our very interaction with the world around us produces a rich set of data that is continually being transmitted and produces an overwhelming amount of information and meta-data about that information. This meta-data, which is practically impossible to protect, includes information about who you are, where you are, who you are communicating or interacting with, the length, frequency, volume and duration of your communications, what applications you are using, and other troves of information.

While much of this information is constitutionally protected from law enforcement collection, they can, and do, legally gain access to this information, including purchasing it from data aggregators. Law enforcement has an overwhelming volume of information readily available to it, creating challenges to efficiently manage and fully leverage it.

The Cloud and New Computing Paradigms Empower and Enable Law Enforcement

In addition to the meta-data overload, law enforcement can now gain access to raw content at an unprecedented level. Business is transforming faster than ever before. Technology has become the key differentiator in just about every industry, and information is the fuel. Technology has enabled businesses to reduce cost, transform and gain competitive advantage.

The present and future belong to the businesses that have the greatest intelligence and can differentiate their insight. By gaining access to a customer's information, or perhaps more importantly the information of a prospective customer, companies can simply comb through such data, a process known as data-mining, and produce the most targeted information of the greatest value. This is a practice that each and every one of our industry leading corporations is utilizing.

The new economy uses information to delight us. The magic of the applications we use and the utility and enjoyment we get from them are not on our computer or mobile devices. The power of modern apps and business transcends our computing platforms and occurs in the cloud.

Application providers process it, and sort the unencrypted information in order to deliver the insight we want. For information efficiency and resiliency purposes, unless you very conscientiously make the deliberate effort to evade it, the majority of content you produce or interact with is accessible in a clear text form by the organization you work for and the companies you engage with in your personal capacity. This makes such information readily accessible to law enforcement operating through proper legal channels.

Keeping Information Secret is Really Hard to Do

Good cryptography is really hard to do well, even when it is readily available; algorithms are only a small part of the puzzle. Flaws are constantly being detected in how algorithms are implemented, in key exchange mechanisms, in shared memory or storage, where keys can frequently be found. Even when good cryptography is readily available, protecting information is

incredibly hard to do. There are inevitably flaws in the other moving parts, such as hardware, protocol implementations, operating systems, authentication mechanisms and other components of the computing platform that can compromise information, even if such information is properly encrypted.

We all read about high profile cyber breaches. Thousands of individual hackers are regularly discovering buying and selling exploits that provide unfettered and complete access to computer systems. Given physical access to a device there are expectations that any credible intelligence service or sophisticated law enforcement agency should be able to gain access to the information that resides on that device. If the FBI is unable to do so, they should prioritize developing this organic technical capability to solve the problem.

Law enforcement has phenomenal access to information on an unprecedented scale and is continually increasing its visibility.

Exceptional Access Encryption Creates Exceptional Exposure

Although law enforcement has access to a wealth of insightful surveillance data already, recent and heinous terrorist acts have reinvigorated calls for *exceptional access* mechanisms. These exceptional access mechanisms would enable specified government entities to access the underlying contents of encrypted data even if a third-party encrypted that data. Simply put, this is a call to create a "back door" to allow law enforcement access to encrypted information.

While this request ostensibly sounds simple, it is not only infeasible to achieve, but it fundamentally weakens the security of the Internet infrastructure upon which we all continuously rely, impacting both national security and public safety.

As with any cryptosystem, the greatest challenges exist in implementation and in maintaining effective operational security. The concept of exceptional access encryption directly conflicts with the fundamental design principles of modern encryption and cybersecurity in several ways:

– *Exceptional access mechanisms increase complexity.*

  As system complexity increases, so too do the risks of a compromise. In their purest form, security and complexity are typically antithetical to each other. The more complex the system the less safe it is. Each time we add a level or layer of complexity, we add potential for vulnerability. Bear in mind that it can take a significant amount of time and vetting before systems are considered to be secure enough in practice. An exceptional access system will therefore require a more significant incubation period.

– *Exceptional access mechanisms incur operational and procedural risks.*

  How would access work? Compromises of even the most sensitive and well-protected systems occur on a regular basis. These are the breaches we see on the news and the world of breaches that we do not even know about. The technical controls and procedures which would be required to govern and audit legitimate access introduce an even greater complexity.

– *Exceptional access mechanisms introduce an extra point of failure.*

  Whoever possesses the capability of gaining exceptional access now carries the largest target on their back. They have a need of the greatest magnitude to safeguard their own infrastructure and protect the exceptional access. We have not seen the government demonstrate this exceptional capability to date. A compromise of the "Exceptional Access" method would compromise the effectiveness of the entire system. The result might be massively destructive to society.

– *Exceptional access mechanisms aren't compatible with authenticated encryption.*

  The idea behind authenticated encryption is not only to preserve the confidentiality of the underlying data, but also to ensure its authenticity and integrity; i.e., it was encrypted only by the person who had knowledge of the encryption key and no one else could have modified the data. Authenticated encryption is considered a best practice when applying encryption techniques.

– *Exceptional access mechanisms aren't compatible with perfect forward secrecy.*

  In other words, if the key is compromised, then all of the data ever encrypted with this key becomes compromised. A more common practice is to negotiate a new key per transaction and use your longer-term key to help ensure the authenticity and integrity of the negotiation process. Each transaction is then encrypted with a fresh key that is discarded shortly after the transaction is completed. An adversary who compromises a given key only learns the contents of a given transaction and not the transactions that preceded it (or any subsequent transactions for that matter).

These are not esoteric or theoretical risks and there are numerous examples of significant systems being exploited as a result of poor cryptographic implementations, even without the added vulnerability of exceptional access. Such "back door" access is significantly more complex and introduces massive additional complexity and risk to our technology infrastructure.

To this end, the entirety of the cryptographic, cyber security, and technology communities has spoken with one unified voice in an unequivocal and unprecedented fashion. Our individual and collective experiences have taught us that from a security perspective, "Exceptional access is an exceptionally terrible idea."

Requiring Exceptional Access Cryptography Would Likely Harm, Not Improve Our National Security, Intelligence, or Public Safety Capabilities.

Very strong cryptography is readily available outside the United States. A recent survey[2] by Bruce Schneier, a fellow at Harvard's Berkman Center for Internet & Society, demonstrates this very fact: of the 619 entities Schneier identified as selling encrypted products, more than 65 percent are based outside of the U.S., and of the products offered by the non-U.S. companies, nearly half are available for free.

[2] Bruce Schneier, Kathleen Seidel, Saranya Vijayakumar, "A Worldwide Survey of Encryption Products", https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf, (February 11, 2016)

Restricting encryption technology in the U.S. will not make these technologies or known cryptographic methods unavailable. Sophisticated adversaries and criminals, anyone capable of impacting our security, will just create or buy encrypted devices abroad. It is highly unlikely that any credible terrorist or foreign intelligence service would ever use technology that was knowingly weakened or that U.S. intelligence or law enforcement agencies have access to.

If U.S.-based organizations lose customers and market share as a result of enabling some form of exceptional access, U.S. agencies would lose significant visibility into that customer's use cases, meta-data and potential for content. Making matters worse, some countries that historically do not cooperate with U.S. law enforcement and intelligence agencies might purposefully become digital safe havens for end users.

The current Director of the National Security Agency, as well as his predecessors, have stated they do not support a national policy requiring exceptional access encryption.

Weakening Encryption Would Catastrophically Weaken our Nation.

Good encryption is a foundational building block for good cyber security. Without the availability of good encryption, those defending vital U.S. networks and systems would be at a massive disadvantage. We live an era where cyber is consistently cited as the single greatest threat to our way of life. The National Intelligence Estimate and repeated testimonies by James Clapper, the Director of National Intelligence, reinforce this point.

How can we justify a policy that would undermine and disadvantage the already challenging and frequently failing efforts of our cybersecurity practitioners and expect them to keep our industries and us safe? The negative impacts would not only affect tech companies, but every industry, including our critical infrastructures, our audit and law firms, power and utilities, automotive, manufacturing, healthcare, banking and financial industries. An exceptional access policy also runs the risk of further harming U.S. interests on an already suspicious post-Snowden world stage.

While I believe the civil liberties and privacy losses would be significant in the presence of exceptional access, I will leave the articulation of those societal trade-offs for others to expound upon.

Technology and Cyber Industry Engagement

I want to acknowledge the many accomplishments of the Department of Commerce in cyber, including updating the privacy framework, enabling better cooperation between the E.U. and the U.S., the continuous assessment of the NIST Cybersecurity Framework developed hand in glove with industry and now being adopted internationally, and the many standards and best practices that enable the cybersecurity community to build interoperable tools.

Likewise, the Department of Homeland Security has been putting forth a genuine effort to collaborate better with industry and is implementing more efficient information sharing mechanisms.

Policy Considerations

I urge caution with any legislation that would require technology companies to weaken security protocols or provide data to law enforcement in an unencrypted format. The Information Technology Industry Council responded to the discussion draft of the "Compliance with Court Orders Act of 2016," by stating:

> Our ability to constantly innovate and deploy strong security technology is key to protecting not just people's privacy, but their security – including their physical security. We must constantly innovate to stay at least one step ahead of those who would do us harm. This proposal would actually freeze in place the technology we need for protection, leaving all of us extraordinarily vulnerable. [3]

Similarly, the Consumer Technology Association (CTA) called the proposed legislation an "overbroad overreaction," stating: "…requiring access to protected communications would defeat the entire purpose of encryption - opening Americans' data to not only the U.S. government, but also hackers, contentious foreign regimes and other bad actors." CTA also stated, "former NSA and CIA director Michael Hayden, former Homeland Security director Michael Chertoff and former NSA director Mike McConnell have spoken out against similar proposals and argue that encrypted devices are an important weapon against terrorism."[4]

As complex and important as this issue is, I am encouraged by the creation of the House Bipartisan Encryption Working Group, which includes members of this committee and the House Judiciary Committee. I believe it is critical for Members to understand all aspects of this debate before putting pen to paper. I would welcome the opportunity to work with the task force as they consider options for ensuring law enforcement has the tools they need to protect us while preserving the benefits of strong encryption.

We also support the Digital Security Commission Act of 2016 (H.R. 4651), which would create a commission of members of the tech community, privacy advocates, and the law enforcement and intelligence communities to work on a solution. Both the Working Group and the Digital Security Commission provide industry, law enforcement, and other stakeholders with a forum to discuss the potential impact of any proposed path forward, legislative or otherwise, and balance their sometimes competing interests.

We also believe it is important for Congress to bear in mind the international precedent that is being set by this discussion. We have already seen a number of countries, including China and France, signal a strong interest in mandating companies create vulnerability in their technology for the purpose of releasing information to them. While these countries have yet to set such a mandate in statute, they are keeping a close eye on the current debate before the U.S. Congress.

As a company, we try to do our part. At RSA Conference, we bring together industry, law enforcement and national security professionals to engage in dialogue and stay abreast of

---

[3] ITI, "ITI Statement on Discussion Draft Regarding Compliance with Court Orders on Encrypted Communications", https://www.itic.org/news-events/news-releases/iti-statement-on-discussion-draft-regarding-compliance-with-court-orders-on-encrypted-communications, (April 8, 2016)

[4] Consumer Technology Association, "Burr-Feinstein Encryption Bill Overbroad and Threatens Privacy, Says CTA", http://www.cta.tech/News/News-Releases/Press-Releases/2016-Press-Releases/Burr-Feinstein-Encryption-Bill-Overbroad-and-Threa.aspx, (April 11, 2016)

relevant cyber security issues and have been doing so for 25 years. The annual RSA Conferences draw tens of thousands of attendees per year, making RSA Conference the world's largest information security event. This February, speakers at the conference included Attorney General Loretta Lynch, Assistant Attorney General John Carlin and FBI Assistant Director of Cyber Division, James Trainor.

Conclusion

In summary, first, this is no place for extreme positions or rushed decisions. The line connecting privacy and security is as delicate to national security as it is to our prosperity as a nation. I encourage you to continue to evaluate this issue and not rush to a solution.

Second, law enforcement has access to a lot of information they need to do their jobs. Data is readily accessible to law enforcement operating through proper legal channels. There is a need for a better strategy to manage the quantity and efficiency of the information and analysis. I would encourage you to ensure that the FBI and law enforcement agencies have the resources and are prioritizing the tools and technical expertise required to keep up with the evolution of technology and meet their important mission as our society's use of technology evolves.

Third, strong encryption is the basis for good cyber security; if we lower the bar there, we expose ourselves even further to those that would do us harm. Exceptional Access increases complexity and introduces new vulnerabilities. It undermines the integrity of internet infrastructure and introduces more risk, not less, to national interests. Creating a "back door" into encryption means creating opportunity for more people with nefarious intentions to harm us. Back doors into encryption will not address advanced threat actors who pose a material threat to our security. Sophisticated adversaries and criminals would not knowingly use methods they know law enforcement could access, particularly when foreign encryption is readily available. Therefore, any perceived gains from exceptional access are overestimated.

Finally, this is a basic principle of economics with very serious consequences. Our standard of living depends on the goods and services we can produce. If we require exceptional access from US-based companies that would make our information economy less secure, the market will go elsewhere. But worse than that, it would weaken our power and utilities, infrastructure, manufacturing, healthcare, defense and financial systems. Weakening encryption would catastrophically weaken our nation.

Simply put, Exceptional Access does more harm than good. This is the seemingly unanimous opinion of the technology industry, academia, national security, as well as all industries that rely on encryption and secured products.

Closing

In closing, I would like to thank Chairman Murphy and Ranking Member DeGette and all members of the committee for their dedication to better understand this complex issue.

I thank you for the opportunity to be here today, and EMC and RSA look forward to working with you and your colleagues in Congress as encryption and cybersecurity topics remain at the forefront of so many policy decisions we face.