STATEMENT OF

CHRIS INGLIS

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

14 JULY 2016

VERSION: 11 JULY 2016/JCI

Thank you, Chairman McCain, Ranking Member Reed, and Members of the Committee. I am pleased to appear before you today to talk about cyber and encryption issues with a specific focus on the challenges to law enforcement caused by encryption.

The issues in play here are technically complex but, more importantly, cut across several distinguished interests that are not easily reconciled. Consistent with its powers under Article I, I believe the Congress will be an essential component of our ability to identify, create and sustain the framework needed to align the various interests in play.

My comments today are derived from twenty-eight years of experience at the National Security Agency working both of its related but distinguished missions: the Information Assurance mission supporting the defense of critical information and networks, and the Signals Intelligence mission which generates foreign intelligence needed to inform the Nation's defense. While I possess technical degrees in engineering and computer science, the majority of my career at the National Security Agency was spent in leadership positions, including seven and one half year's service as NSA's senior civilian and Deputy Director during the period 2006-2014.

In my opening remarks, I would like to cover three areas:

- First, I think it is important to lay out the framework of interests that can guide choices about desired, or unwanted outcomes that transcend the technology discussions that have so often dominated this debate.

- Second, I will offer my view on the context of encryption within the systems-of-systems we once referred to as the telecommunications sector and now variously refer to as the internet or cyberspace. There are, of course, surgical applications of encryption that can be considered in isolation but these tend to be the exception rather than the rule, even if they are considerably more tractable in sorting out desired outcomes and equities.

- Finally, I will suggest some implications of this discussion in the context of an increasingly interconnected world – one where it is unlikely that purely national solutions will either be acceptable or widely adopted.

Framing the issues in play:

In trying to simplify and untangle the various threads of this discussion, it is tempting to immediately focus on the technology, and more particularly encryption. One of the perils of that approach is that it fails to first establish a foundation of principles and objectives that can drive the attributes of technology and other systems intended to serve the interests of society.

There are arguably at least four interests converging here.

- The first is the desire by individuals for security of the communications and data they transmit across or store on digital devices and networks. This interest is often over-simplified as the desire to protect the ***confidentiality*** of data communicated across or stored in cyberspace – sometimes short-handed as "protecting privacy". But the services

of ***integrity*** and ***availability*** are often just as important – delivering needed confidence to the integrity and resilience of financial transactions, personal preferences, and the flow of critical resources ranging from energy to airplanes. Encryption technology can and does make a contribution to all three of the basic security services, transcending the issue of privacy alone.

- The second interest in play here is the goal of protecting society from the actions of those who would use internet based communications to plan, coordinate or deliver harm to its collective security interests. These threats include but are not limited to the use of internet based communications to conduct illicit activity such as child pornography, terrorism, or the delivery of cyber threats. Indeed, it is the demonstrated potential for encryption to provide anonymity and cover to those who threaten our collective interests that underpins law enforcement's and the intelligence community's desire to gain access to the contents of individual communications.

- The third interest in play here is the desire of individuals or companies to freely innovate, create, share and sell products in the marketplace without interference from government. Their ability to do so is, of course, a vital a component of US freedoms and its economic and national security.

- Building upon the third interest, a fourth interest emerges, namely the need for US companies to remain competitive in what has become a ***global*** marketplace, a desire that is particularly acute for companies doing business across differing legal regimes where the balance struck between privacy and collective security is uneven. Solutions that arbitrarily deliver unique advantage to one society above others will falter and fail in that world, risking not only a company's viability in foreign markets but the economic vitality and prosperity of the US itself.

Taken individually, each of these aims can be viewed as a laudable goal. Taken in sum, an unqualified commitment to one of the aims necessarily makes it more challenging to achieve one or more of the others. Further, the dynamic nature of technology and its creative application to myriad tasks by millions of users greatly increases the difficulty of striking and sustaining a particular balance over time. Keeping up with this ever changing landscape has always been a challenge for the conduct of lawful surveillance by law enforcement or intelligence agencies. This is generally referred to by the law enforcement community as "going dark". Encryption is only one component of this challenge.

In any event, unless, and until, we determine which of these interests we want to support, we will be unable to judge the efficacy and suitability of any particular system, technology, or protocol.

Some would argue that these four interests constitute a choice. I believe this is shortsighted. The US Constitution provides useful guidance here in its use of the word "**and**", not "**or**" as the conjunction joining the preamble's enumeration of goals motivating the formation of a "more perfect union": *"to provide for the common defence, promote the general Welfare, **and** secure the Blessings of Liberty to ourselves"*.

I am firmly convinced that the innovation, creativity and industry exist to align and support all four of the interests I've outlined here. Whatever the choice may be, the premise of our union is that we must establish the overarching goal before devising laws, procedure and technologies that advance those stated interests.

On the nature of "secure systems"

There are two common misconceptions that often cloud this debate. The first is that encryption stands on its own as a security tool. In practice, across the vast majority of security systems, encryption is just one of several mechanisms used in combination to deliver the desired mix of confidentiality, availability and integrity. To be sure, encryption is an increasingly **essential** component of a globally deployed security system, protecting both data in motion and at rest, but it is hardly ever sufficient in and of itself. Physical security, personnel security, user behaviors, and hardware and software security are all equally essential components. This observation is not meant to detract from a necessary focus on the resilience of encryption schemes but we should not fool ourselves that a strong right arm on an otherwise underdeveloped frame is enough to protect our interests. This will be ever truer as technology continues to advance. By way of example, the possibility of quantum computing should remind us that our focus should be on determining principles that will endure across the inexorable roil of technology transformation.

The second, and more important, misconception about encryption is that it's a monolithic thing. That you either have it "on" or you don't.

A quick look at the diversity of user expectations and vendor choices reveals that it's far more nuanced and complicated.

Some users want their data encrypted so that only they can recover it. No vendor backups. No emergency recovery service. No possibility of third party access or government surveillance.

Other users want a safety net – the ability to recover a lost key, or retrieve lost data by backing it up on some medium, say the "cloud", that's recoverable under a variety of circumstances.

More significantly, vendor choices regarding their service offerings cater to this broad array of user preferences while adding an overlay of vendor preferred attributes. Some vendors deliver encryption systems that cannot be penetrated by the vendor, either for its own purposes, or on behalf of others, whether that's the user or the government. Other vendors build and deliver systems that contain "exceptional access mechanisms" – built-in means to remove the overlay of encryption at various points in the transport or storage of a piece of data. The commercial reasons for this "exceptional access" run the gamut from creating safety nets for users seeking to recover data when they cannot remember or find their encryption keys, to enabling access to data by a party other than the data owner for the purpose of analyzing user content to tee up targeted advertising or other commercial offerings.

The result is an architectural landscape where some vendors place security controls wholly in the hands of the user while others deliver systems that allow the vendor, or third parties, to access user data because that access is essential to the vendor's business model. These differing

approaches are not generally portrayed as weak versus strong encryption. They are more properly differentiated by their choice of how and when the protected materials may be revealed.

This diversity of choices reflects the reality of a free market economy and the rights of individuals, including companies, to pursue features of their own preference. As such, these choices are neither good nor bad. They're just choices. Moreover, this diversity in approach suggests that there is no one design principle driving the use of encryption, and most certainly there is no one way to make good use of it. But if we assume that these same market forces will deliver a principled reconciliation, if not an alignment, of societal goals that will endure over time, diverse user expectations, and attendant technology transformation we need only observe the diversity of choices currently available, or remember the excesses periodically delivered by markets seeking private advantage for some company or segment of the private sector.

In the face of this natural diversity in architectural choices, the use of terms like "backdoors" and "secret keys" must be seen as pejorative and unhelpful. If it is ultimately determined by system designers that it is appropriate to provide a means for exceptional access for some party other than the data owner, the important questions will be: "Is there a legitimate purpose being served?" "Does the data owner understand the nature, if not the details, of the potential access?" and "Are the controls on the access sufficient to ensure such access is constrained to the identified purpose and not abused?"

Summarizing:

I will summarize my opening remarks by enumerating the key implications suggested by them:

First, the use of strong encryption is an essential component of security for our nation and our citizens. The fundamental question in such systems is how access to stored or transmitted data is controlled by the application of strong encryption.

Second, a framework to reconcile the various interests arguing for potentially different technical solutions in this debate will be best served by first reconciling, if not aligning, our societal goals before considering a particular implementation offered by one or more vendors, the government, or subject matter experts.

Third, if our goal is to deliver security for individuals, ***and*** security for the American people writ large, ***and*** continued economic vitality in a global marketplace for American industry then our framework must align and deliver these three goals in a global context, neither surrendering nor wholly favoring US security to the detriment of like-minded Nations.

Fourth, it is considerably more likely that law enforcement interests can be parsed into international norms than can national security interests. A bias towards law enforcement's interests in this area may be appropriate to deliver a framework and attendant solutions that work across national boundaries and to address the more pressing needs of local law enforcement, which often lack the technical resources to pursue other means of accessing data pursuant to a lawful investigation.

Fifth, market forces, alone, have seldom shown themselves able to deliver a consistent alignment of societal outcomes across the diverse products and services of vendors at any time, and have never delivered one across time.

Finally, in as much as I describe a mandate for government action in this space, I think government action must be:

- Fully informed by the various interests government is formed to represent;
- Focused on ensuring the various freedoms and rights of individual citizens while also maintaining collective security;

and

- Mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government both in facilitating the creation of an enduring, values based, framework that will drive technology and attendant procedures to serve society's interests, and in reconciling that framework to-and-with like-minded Nations in the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preferences of other nation-states which will drive, unopposed, solutions that we are likely to find far less acceptable.

In that spirit, I applaud the initiative and further work of this committee in taking up the matter and working through these difficult issues.

I look forward to your questions.