Testimony by Herbert Lin
Senior Research Scholar, Center for International Security and Cooperation
Research Fellow, Hoover Institution
Stanford University
Chief Scientist (Emeritus), CSTB, National Academies

Senate Judiciary Committee
July 8, 2105

Ladies and Gentlemen, thank you for inviting me to testify today. I have worked on cyber policy and security issues for many years, mostly at the National Academies and now at Stanford University, but the views I present today are my own.

The previous panel discussed "going dark", and I want to address 3 issues.

- First, the US government has framed solutions to the "going dark" problem around the concept of NOBUS access to encrypted data. (NOBUS stands for "nobody but us" where "us" is the government, a term first used publicly by Michael Hayden.) This approach has generated polarization around two positions. One side says NOBUS access inevitably weakens the security of a system and will eventually be compromised by a bad guy; the other side says it doesn't weaken security and won't be compromised. Neither side can **prove** its case, and we see a theological clash of absolutes.

  To get out of this box, let's instead consider time scale. If it takes a thousand years for a bad guy to figure out how to hack a NOBUS mechanism, that's probably secure enough. If it takes him 30 seconds, using that mechanism is a dumb idea. So somewhere between 30 seconds and a thousand years, the mechanism changes from being unworkable to being secure enough.

  How can we estimate the time the bad guy needs? We don't understand very well today how to make these estimates for computer systems. But there are methodologies that are often used today to make such estimates for systems in other domains. For example, an approach called **probabilistic risk analysis** is often used in estimating the time before a nuclear reactor experiences a meltdown. Generally speaking, one estimates the probabilities of various sequences of events that could lead to failure-- what's called fault and event tree analysis, and out of that comes an estimate that it will take 10,000 years or a million years. Opponents and proponents of nuclear power use different numbers to make their estimates, but at least they use the same methodology and they can identify where they disagree technically. That's a better outcome than shouting at each other over a table saying "yes" or "no".

  The most important thing about this approach is that it requires a specific reactor design and siting plan to analyze. Only when specifics are involved can one actually have a technical debate.

  Would a similar approach work in analyzing a proposed NOBUS mechanism? I think so, but I could be wrong. That's why it's a research problem—we should assess whether such methodologies can be usefully applied to estimate how long it might take for a bad guy to hack any specific NOBUS mechanism. But the government has not yet provided any specifics, arguing

that private vendors should do it. At the same time, the vendors won't do it, because its customers aren't demanding such features. Indeed, many customers would see such features as a reason to avoid a given vendor.

Without specifics, there will be no progress. I believe the government is afraid that any specific proposal will be subject to enormous criticism—and that's true—but the government is the party that wants NOBUS access, and rather than running away from such criticism, it should embrace any resulting criticism as an opportunity to improve upon its initial designs and provide a proof of principle that the approach is possible.

Exactly the same issues came up in the 1990s, only then the government did propose a specific mechanism. When the National Academies studied the problem then, it made a recommendation that still makes sense today—a pre-requisite for going down this path is for the government to gain experience about how to properly operate a government-only system allowing NOBUS access. Without such experience, large scale deployment of any access mechanism across the entire nation is asking for trouble.

A final point is asking the major vendors to provide NOBUS access is only the first step, as Director Comey implied in his comments regarding end-to-end encryption to CNN on June 18. The next step is to impose access requirements on small app and open source developers, because they can build apps that bypass NOBUS mechanisms built into the platforms. And then you have to prevent people from bringing into the U.S. apps from abroad that don't have NOBUS access, which means an Internet firewall around the United States that blocks such apps and border inspections and import controls.

- Second, a partial alternative to NOBUS access is for law enforcement authorities to obtain legal authorization to take advantage of the vulnerabilities that already exist in all software. With proper legal authorization, law enforcement could hack the devices of bad guys to obtain unencrypted information when the bad guys themselves accessed it, and they do this to some extent today.

- Third, criminals are just like the rest of us in that they also forget passwords, and if they have not saved them somewhere, certain crimes will not happen because the would-be perpetrators will not be able to get the information needed to commit them. Remember also that data is often backed up to the cloud by default. So criminals will want mechanisms that enable them to retrieve inaccessible data, and if they do, that's a way that law enforcement can gain access.

I hope that these comments are helpful and I'm ready to answer questions. I ask that a number of relevant documents that support my testimony be entered into the record. These documents have already been provided to Committee staff.

Documents for the record

- Executive summary to 1996 NRC report: Cryptography's Role in Securing the Information Society

  Motivated in part by the U.S. government proposal to promulgate escrowed encryption and the Clipper chip as a solution to the "going dark" problem of the 1990s, this report provided an analysis of escrowed encryption that is a useful point of departure for understanding today's debate. The recommendation that the government gain experience in operating an escrowed encryption system in its own domain (government systems and applications) is discussed in this report.

- Blog post from Herb Lin - http://www.lawfareblog.com/making-progress-encryption-debate, http://www.lawfareblog.com/echoes-past-encryption.

  The "Making Progress" blog post discusses my argument that the time needed to compromise a NOBUS mechanism is what matters to this debate. The "Echoes" post makes the point about criminals forgetting passwords too.

- Blog post from Jonathan Mayer- http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform/

  The Mayer blog post describes the "first step" argument in greater detail.

- Bellovin et al-"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

  The Bellovin et al paper makes the case that lawful hacking is a way for law enforcement authorities to gain much of the access they need without introducing additional security vulnerabilities.

- Blog post from Paul Rosenzweig - http://www.lawfareblog.com/encryption-wars-continue.

  The Rosenzweig blog post elaborates the argument about default backup of data to the cloud.