Oral Statement of Kevin S. Bankston
Policy Director of New America's Open Technology Institute
& Co-Director of New America's Cybersecurity Initiative

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

Hearing on "Encryption Technology and Possible U.S. Policy Responses"

April 29, 2015

Thank you, Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee.

District Attorney Conley is absolutely right: encryption is one of the most critical law and order issues of our time. However, and with respect and thanks for his and the FBI's work to keep us all safer, he's got it exactly backward: strong encryption is absolutely critical to the preservation of law and order in the digital age, much more than it is a threat to it.

Some have framed this debate as a choice between safety and privacy. But that's a false choice. The debate over whether to allow strong encryption without backdoors is really a choice between safety and safety—a little more safety against some isolated crimes, or much more safety, for many more people, against countless other concrete criminal and national security threats—be they street criminals looking to steal our phones and laptops, ID thieves and fraudsters and Russian hackers and corporate spies trying to steal our most valuable data, or foreign intelligence agencies trying to compromise our most sensitive national security secrets.

The ultimate question isn't, what will make law enforcement's job easier in some investigations. The ultimate question is what will prevent more crime—which will make law enforcement's job easier overall, and will keep us all safer. The answer to that question is more strong encryption, not less.

I won't deny that encrypted devices or end-to-end encrypted communications will, in some cases, inconvenience law enforcement. Notably, however, the government has yet to provide a single specific example where such encryption has posed an insurmountable problem. That's likely because there are often a variety of other ways for law enforcement to get the evidence it needs. The FBI is concerned that it's going dark, but all in all, the digital revolution has been an enormous boon to law enforcement—what some have called a "golden age of surveillance."

More and more of our interactions with others and with the world are moving into the digital realm, being quantified and recorded—an unprecedented and exponentially growing cache of sensitive data about all of us, and most of it available to law enforcement.

Think about the massive archives of private email and instant messages and text messages and photos and videos, and the vast records of our social network activities, most of which didn't exist or weren't available just fifteen years ago, most of which are stored in the Internet cloud and easily accessible to law enforcement, and much of which is backed up from the very same encrypted phones that the government is concerned about. Think of all of the new metadata revealing when and with whom all of those messages were exchanged, where and when those photos and videos were taken. And think especially about all of that new location data generated by our cell phones and by our mobile apps, creating extensive records of our movements regardless of whether those phones are encrypted or not.

Think about all of that when law enforcement says it is going dark. I would counter that by most measures, they are going bright.

And in those few cases where they are in the dark, and they truly need the data on an encrypted device—even then, there are options. They can in many cases ask the court to compel the owner to decrypt the device under threat of contempt—or even remotely hack into the device over the Internet, a technique that's being used more and more often. Admittedly, I have some serious constitutional concerns about both of those law enforcement techniques. But I am much more concerned that in order to address those rare cases, law enforcement seems to want Congress to take steps that would undermine everyone's security, rather than targeting an individual suspect.

And make no mistake—attempting to mandate encryption backdoors will undermine everyone's cybersecurity, as Professor Blaze will testify. That is the unanimous conclusion of every technical expert that has spoken publicly on this issue. And as Mr. Potter will make clear, surveillance backdoor mandates would also undermine our economic security and prompt international customers—and many American consumers—and even many of the bad guys that we're trying to stop—to turn away from the compromised products and services offered by U.S. companies.

It's true now, just as it was true in during the so-called "Crypto Wars" of the 90s: weakening encryption is a bad idea. That is why a majority of the House of Representatives at the time—including four current members of this Oversight Committee including Ranking Member Cummings—cosponsored Chairman Goodlatte's Security and Freedom Through Encryption Act, which would have reaffirmed Americans right to make, use and distribute strong encryption products without backdoors. That is why a majority of the House just last year voted for the Sensenbrenner-Massie-Lofgren amendment that would have prohibited the NSA from demanding or even asking that companies weaken the security of their products. And that is why this Congress should similarly reject any shortsighted backdoor proposals in favor of preserving our long-term national and economic security.

Thank you and I look forward to your questions, including any questions about the ten specific arguments offered in my written testimony.