STATEMENT OF BRUCE SCHNEIER

Energy & Commerce Committee hearing November 16th, 2016

Mr. Schneier.

Thank you, Chairman Walden, Chairman Burgess, Ranking Members Eshoo and Schakowsky. Committee members, thank you for having me and thank you for having this, I think, very important hearing.

I am Bruce Schneier. I am a security technologist. And while I have an affiliation with both Harvard and IBM, I am not speaking for any of them and I am not sure they know I am here.

Mr. Walden. It is a secret. Nobody on the Internet knows either.

Mr. Schneier. As the chairman pointed out, there are now computers in everything, but I want to suggest another way of thinking about it, in that everything is now a computer. This is not a phone, this is a computer that makes phone calls; or a refrigerator is a computer that keeps things cold; an ATM machine is a computer with money inside. Your car is not a mechanical device with computers, but a computer with four wheels and an engine, actually, a hundred computer distributed system with four wheels and an engine. And this is the Internet of things, and this is what caused the DDoS attack we are talking about.

I come from the world of computer security, and that is now everything security. So I want to give you four truths from my world that now apply to everything.

First, attack is easier than defense for a whole bunch of reasons.

The one that matters here is that complexity is the worst enemy of security. Complex systems are hard to secure for an hour's worth of reasons, and this is especially true for computers and the Internet.

The Internet is the most complex machine mankind has ever built by a lot and it is hard to secure. Attackers have the advantage.

Two, there are new vulnerabilities in the interconnections. The more we connect things to each other, the more vulnerabilities in one thing affect other things. We are talking about vulnerabilities in digital video recorders and Web cams that allowed hackers to take down Web sites. There are stories of vulnerabilities in a particular account.

One story. A vulnerability in an Amazon account allowed hackers to get to an Apple account, which allowed them to get to a Gmail account, which allowed them to get to a Twitter account. Target Corporation, you remember that attack. That was a vulnerability in their HVAC contractor that allowed attackers to get into Target. And vulnerabilities like these are hard to fix because no one system might be at fault. There might be two secure things come together and create insecurity.

Truism three:

The Internet empowers attackers, attack scale.

The Internet is a massive tool for making things more efficient, and that is also true for attacking. The Internet allows attacks to scale to a degree impossible otherwise. We are talking about millions of devices harnessed to attack Dyn, and that code, which somebody smart wrote, has been made public. Now anybody can use it. It is in a couple of dozen botnets right now. Any of you can rent time on one on the dark Web to attack somebody else. I don't recommend it, but it can be done. And this is more dangerous as our systems get more critical.

The Dyn attack was benign, a couple of Web sites went down. The Internet of things affects the world in a direct and physical manner:

Cars, appliances, thermos tats, airplanes. There are real risks to life and property and there are real catastrophic risks.

The fourth truism: The economics don't trickle down. Our computers are secure for a bunch of reasons. The engineers at Google, at Apple, at Microsoft spent a lot of time at this, but that doesn't happen for these cheaper devices. Ms.Eshoo has talked about this.

These devices are lower profit margin, they are offshore, there are no teams, and a lot of them cannot be patched. Those DVRs, they are going to be vulnerable until someone throws them away, and that takes a while. We get security, because I get a new one of these every 18 months. Your DVR lasts for 5 years, your car for 10, your refrigerator 25. I am going to replace my thermostat approximately never.

So the market really can't fix this. The buyer and seller don't care. And Mr. Burgess pointed this out. The buyer and seller want a device that works. This is an economic externality. They don't know about it and it is not part of the decision. So I argue that government has to get involved, that this is a market failure, and what I need

are some good regulations. And there is a list of them, and Dr Fu is going to talk about some of them, but this is not something the market can fix.

And to speak to Mr. Walden's point, I mean, yes, I am saying that a U.S. only regulatory system will affect the products in the world, because this is software. Companies will make one software and sell it everywhere, just like, you know, automobile emissions control laws in California affect the rest of the country. It makes no sense for anybody to come up with two versions. And I think this is going to be important, because for the first time, the Internet affects the world in a direct and physical manner.

And the second point I want to make very quickly is we need to resist the FBI's calls to weaken these devices in their attempt to solve crimes. We have to prioritize security over surveillance. It was okay when it was fun and games, but now, you know, already this stuff on this device that monitors my medical condition, controls my thermostat, talks to my car, I mean, I have just crossed four regulatory agencies and it is not even 11 o'clock. This is going to be something that we are going to need to do something new about.

And like many new technologies in the 20th century, new agencies were created: Trains, cars, airplanes, radio, nuclear power. My guess is this is going to be one of them, and that is because this is different. This is all coming. Whether we like it or not, the technology is coming. It is coming faster than we think.

I think government involvement is coming, and I would like to get ahead of it. I would like to start thinking about what this would look like.

And we are now at the point, I think, where we need to start making moral and ethical and political decisions about how these things worked.

When it didn't matter, when it was Facebook, when it was Twitter, when it was email, it was okay to let programmers, to give them the special right to code the world as they saw fit. We were able to do that. But now that it is the world of dangerous things, that is, cars and planes and medical devices and everything else, that maybe we can't do that anymore. And I don't like this. I like the world where the Internet can do whatever it wants whenever it wants at all times. It is fun. This is a fun device. But I am not sure we can do that anymore.

So thank you very much, and I look forward to questions.