Testimony of Bruce Schneier
Fellow, Berkman-Klein Center at Harvard University
Lecturer and Fellow, Harvard Kennedy School of Government
Special Advisor to IBM Security and CTO of Resilient: An IBM Company

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology, and the
Subcommittee on Commerce, Manufacturing, and Trade

Joint Hearing Entitled
"Understanding the Role of Connected Devices in Recent Cyber Attacks"

November 16, 2016
10:00 AM

Good morning. Chairmen Walden and Burgess, Ranking Members Eshoo and Schakowsky, members of the committee: thank you for the opportunity to testify on this matter. Although I have an affiliation with both Harvard University and IBM, I am testifying in my personal capacity as a cybersecurity expert and nothing I say should be construed as the official position of either of those organizations.

I have worked in Internet security since the mid-1990s. I write books, articles, essays, and academic papers. I teach at the Harvard Kennedy School of Government. I give talks all over the world. I have testified before Congress before, and have served on several national and international committees on these topics.

Last month, popular websites like Twitter, Pinterest, Reddit and PayPal went down for most of a day. The distributed denial-of-service attack that caused the outages, and the vulnerabilities that made the attack possible, was as much a failure of market and policy as it was of technology. If we want to secure our increasingly computerized and connected world, we need

more government involvement in the security of the “Internet of Things” and increased regulation of what are now critical and life-threatening technologies. It’s no longer a question of if, it’s a question of when.

First, the facts. Those websites went down because their domain name provider — a company named Dyn — was forced offline. We don’t know who perpetrated that attack, but it could have easily been a lone hacker. Whoever it was launched a distributed denial-of-service attack against Dyn by exploiting a vulnerability in large numbers — possibly millions — of Internet-of-Things devices like webcams and digital video recorders, then recruiting them all into a single botnet. The botnet bombarded Dyn with traffic, so much that it went down. And when it went down, so did dozens of websites.

DDoS attacks are neither new nor sophisticated. The attacker sends a massive amount of traffic, causing the victim’s system to slow to a crawl and eventually crash. There are more or less clever variants, but basically, it’s a datapipe-size battle between attacker and victim. If the defender has a larger capacity to receive and process data, he or she will win. If the attacker can throw more data than the victim can process, he or she will win.

The attacker can build a giant data cannon, but that's expensive. It is much smarter to recruit millions of innocent computers on the internet. This is the “distributed” part of the DDoS attack, and pretty much how it’s worked for decades. Cybercriminals infect innocent computers around the internet and recruit them into a botnet. They then target that botnet against a single victim.

You can imagine how it might work in the real world. If I can trick tens of thousands of others to order pizzas to be delivered to your house at the same time, I can clog up your street

and prevent any legitimate traffic from getting through. If I can trick many millions, I might be able to crush your house from the weight. That's a DDoS attack — it's simple brute force.

Because of these attacks, your security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you've never heard of to consumers who don't care about your security.

I want to focus on the particulars of this attack, but the general vulnerabilities from these Internet-of-Things devices. In many ways, the Dyn attack was benign. Some websites went offline for a while. No one was killed. No property was destroyed. But computers have permeated our lives. The Internet now affects the world in a direct physical manner. The Internet of Things is bringing computerization and connectivity to many tens of millions of devices worldwide. We are connecting cars, drones, medical devices, and home thermostats. What was once benign is now dangerous.

Insecurities abound. It is no longer surprising when security researchers demonstrate that cars can be disabled remotely over the Internet. We have seen ransomare against Internet-enabled thermostats, and hacks against computerized medical devices. We know that our computerized election machines are insecure, and that we can be eavesdropped on through our Internet-enabled televisions. These devices are proliferating, and they're vulnerable.

The technical reasons that Internet-of-Things computers are insecure is complicated, but there is a fundamental market failure at work. Basically, the market has prioritized features and cost over security. Many of these devices are low-cost, designed and built offshore, then rebranded and resold. The teams building these devices don't have the security expertise we've come to expect from the major computer and smartphone manufacturers, simply because the market won't stand for the additional costs that would require. Unlike your computer and

smartphone, these devices don't get security updates, and many don't even have a way to be patched. And, unlike our computers and phones, they stay around. DVRs and cars last a decade. Refrigerators, twenty-five years. We expect to replace our home thermostats approximately never.

This is important. The vulnerability exploited in the Dyn attack was made public, and is now in over a dozen different botnets. There is no way to patch the CCTV cameras and DVRs that are being exploited, and those devices will remain on the Internet for years if not decades.

They'll remain in use because of an additional market failure: neither the seller nor the buyer of those devices cares about fixing the vulnerability. The owners of those devices don't care. They wanted a webcam — or thermostat, or refrigerator — with nice features at a good price. Even after they were recruited into this botnet, they still work fine — you can't even tell they were used in the attack. The sellers of those devices don't care: They've already moved on to selling newer and better models. There is no market solution because the insecurity primarily affects other people. It's a form of invisible pollution.

And, like pollution, the only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers, allowing companies like Dyn to sue them if their devices are used in DDoS attacks. The details would need to be carefully scoped, but either of these options would raise the cost of insecurity and give companies incentives to spend money making their devices secure.

Most importantly, the government needs to resist the urge to deliberately weaken the security of any computing devices at the request of the FBI. Devices like smart phones are becoming the de facto digital hub where we control many of our Internet-of-Things devices.

Attempts to weaken encryption will make these attacks easier and more damaging, and will harm our society far more than their benefit to FBI investigations. Invest in FBI cybersecurity expertise, not back doors.

It's true that this is a domestic solution to an international problem and that there's no U.S. regulation that will affect, say, an Asian-made product sold in South America, even though that product could still be used to take down U.S. websites. But the main costs in making software come from development. If the United States and perhaps a few other major markets implement strong Internet-security regulations on IoT devices, manufacturers will be forced to upgrade their security if they want to sell to those markets. And any improvements they make in their software will be available in their products wherever they are sold, simply because it makes no sense to maintain two different versions of the software. This is truly an area where the actions of a few countries can drive worldwide change.

Regardless of what you think about regulation vs. market solutions, I believe there is no choice. Governments will get involved in the IoT, because the risks are too great and the stakes are too high. Computers are now able to affect our world in a direct and physical manner.

Security researchers have demonstrated the ability to remotely take control of Internet-enabled cars. They've demonstrated ransomware against home thermostats and exposed vulnerabilities in implanted medical devices. They've hacked voting machines and power plants. In one recent paper, researchers showed how a vulnerability in smart lightbulbs could be used to start a chain reaction, resulting in them *all* being controlled by the attackers — that's every one in a city. Security flaws in these things could mean people dying and property being destroyed.

Nothing motivates the U.S. government like fear. In 2001, a small-government Republican president created the Department of Homeland Security. A fatal IoT disaster will

similarly spur our government into action, and it's unlikely to be well-considered and thoughtful action. Our choice isn't between government involvement and no government involvement. Our choice is between smarter government involvement and stupider government involvement. We have to start thinking about this now. Regulations are necessary, important and complex — and they're coming. We can't afford to ignore these issues until it's too late.

Letting the market figure out optimal security levels was okay when software didn't matter. But it is fundamentally different when a spreadsheet crashes and you lose your data and when your car crashes and you lose your life. The security vulnerabilities in the Internet of Things are deep and pervasive, and they won't get fixed if the market is left to sort it out for itself. We need to proactively discuss good regulatory solutions; otherwise, a disaster will impose bad ones on us.