Statement of Ranking Member Frank Pallone, Jr.
Energy and Commerce Committee
Commerce, Manufacturing, and Trade Subcommittee
Hearing on "The Internet of Things: Exploring the Next Technology Frontier"
March 24, 2015

Thank you, Chairman Burgess. Today's hearing gives us an opportunity to look at a new and evolving technological development. The Internet of Things has great potential for growing the American economy and offering consumers new technology that will enrich their lives and empower them in ways never before thought possible.

Earlier today, along with my colleagues, I had an opportunity to see some of the innovation coming out of the Internet of Things at a showcase hosted by the Subcommittee. I was proud to have there, iMPak Health, a New Jersey company that is building wireless technology into products to solve practical health care needs. iMPak Health is taking advantage of wireless technology to help ensure patients are taking their medication and staying healthy.

The growth in these types of devices is so rapid that they soon will be as ubiquitous as electrical outlets. In fact, it is estimated that there will be 50 billion connected products by 2020.

But in many ways, the future is already here. Just last Friday, Tesla announced that it would remotely install software updates in its Model S cars providing them with capability of autonomous driving. Cars that drive themselves were once only found in science fiction, but today it can be reality with a quick update sent over the Internet.

Yet, along with these innovations come new vulnerabilities—vulnerabilities that we in Congress have a responsibility to protect consumers against.

Let's take a hypothetical situation for a moment. Let's say that I wear a bracelet that monitors different aspects of my health and physical activity. It helps me keep track of how many steps I take each day, it tells me how well I sleep at night, it monitors my heartrate, and along with an app in my phone, it tracks where I have gone.

While all of this data is important to me, I may not want to have to release it to a potential employer who requires it as part of the job application. I may not want the bracelet manufacturer selling it to an insurance company who might then utilize it for my insurance coverage. And I certainly do not want a hacker accessing the bracelet to post my information on the Internet or to monitor my location.

Without strong security and privacy protections, consumers can be at real risk. These risks can have devastating consequences when the product is accessed and controlled remotely by an unscrupulous actor. One hacker has shown that he can remotely access an insulin pump and induce a lethal overdose. Others have shown that they can remotely hijack the operations of a car, suddenly turning the wheel or cutting off the brakes.

In order to protect consumers, there has to be strong security and privacy protections built into these products.

By "building-in" security, manufacturers can more effectively prevent hackers from accessing a device or the data it produces or collects. At last week's hearing, the Federal Trade Commission's witness stated that its experience in evaluating the vulnerability in Internet of Things products has led to the agency recommending that device security be added to data security and breach notification legislation.

By "building-in" privacy, consumers can have confidence in these products. Consumers need to know that their intensely personal information will not be shared with the world without their consent.

I am confident great things will be done through the Internet of Things. But I believe that while we encourage innovation through these new technologies, we also must be innovative in how we protect the consumer.