COMMITTEE ON DEMOCRATS
ENERGY & COMMERCE
RANKING MEMBER FRANK PALLONE, JR.

FOR IMMEDIATE RELEASE
March 3, 2016

CONTACT
Christine Brennan — (202) 225-5735

Statement by Ranking Member Frank Pallone, Jr., as prepared for delivery
House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade
Hearing on "Disrupter Series: Wearable Devices"

Thank you, Chairman Burgess. Today's hearing gives us an opportunity to look at a diverse and quickly developing field.

Wearable technology—part of the broader Internet of Things—provides consumers with capabilities that would have seemed more like science fiction than reality only a decade ago. Today, you can buy a wristband that measures UV exposure, helping you avoid sun damage or a sensor that sticks to skin and teaches you how to stretch to alleviate back pain. Or smart shoes that give you directions through buzzes to their feet.

Researchers from WINLAB—the Wireless Information Network Laboratory—at Rutgers University in my district, collaborated to design a wearable that could replace passwords for head-worn devices by authenticating the user by measuring the unique movements of the head in response to audio stimulus. WINLAB reports that the device can accurately tell that the right person is wearing it at a rate of over 95 percent through tiny movements of the head alone.

Many wearables measure biometric data, giving consumers access to a wealth of personal information. Not too long ago, if someone wanted to know their heart rate, quality of sleep, and calories burned, they would have had to be hooked up to a room full of equipment. Today, they can simply put on a small bracelet and have all of that information at their fingertips.

These are amazing advancements, but with these new innovations come new vulnerabilities. For example, when a doctor measures your heart rate, that information is protected from unauthorized disclosure. Those privacy protections do not apply to the same information collected through most wearable devices. And there are no standards for encryption or other security measures to protect the data wearables collect.

Long and complicated user terms and agreements have further compounded the problem. Some include clauses saying that the data they collect belongs to the company, not to the user. Most of us do not read every online user agreement word for word, so many wearables users are surprised when they learn that they may not own their own data.

Whether by sale or by data breach, the release of personal information from wearables can have serious implications. Employers, credit agencies, and health insurers can all use the data collected from wearables to draw inferences that may have a negative effect on the user.

As with other Internet of Things products, by building in security from the beginning, manufacturers of wearables can more effectively prevent hackers from gaining access to a device or the data it collects. By building in privacy, consumers can have confidence in these products, and buy them knowing that highly personal information will not be shared without their consent.

I look forward to discussing the many great innovations in wearable technology today. But with these innovations we must also devote serious attention to how we can better protect consumers and their personal information in this space. When privacy and security are made a priority, both businesses and consumers benefit.

###