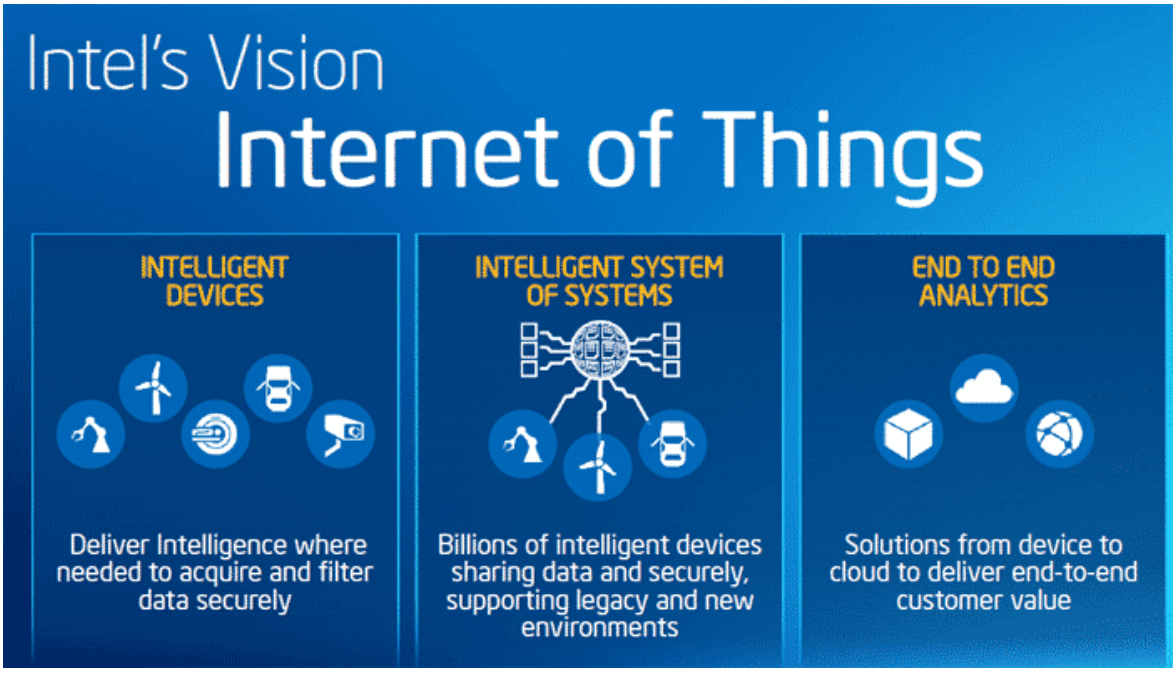

Privacy Concerns Grow As IoT Devices Light Up

The great majority of citizens do not trust the Internet of Things for two big reasons: lack of security and data privacy. Technocrats won't correct this without legally mandated legislation. TN Editor

The safety and security of internet of things (IoT) devices remains a vexing issue for lawmakers, while a survey from the Internet Society shows there is still some way to go before reaching widespread public acceptance of IoT connectivity.

The survey, conducted in six countries by polling firm IPSOS Mori, found that 65% of those surveyed are concerned with how connected devices collect data, while 55% do not trust those devices to protect their privacy. Meanwhile, 63% of those surveyed said they find IoT devices, which are projected to number in the tens of billions worldwide, to be "creepy."

Those concerns were at the forefront of a hearing last week on IoT security by the U.S. Senate Committee on Commerce, Science and Transportation's Subcommittee on Security, where lawmakers and witnesses debated how to make the devices safer and more transparent

for consumers, and what the role of the federal government should be in legislating that. It's a dilemma for policymakers and industry leaders who must wrestle with these questions.

"We can't put the genie back in the bottle," Internet Society president and CEO Andrew Sullivan told Smart Cities Dive. "We have invented this technology, so we're going to have to figure out how to cope with it now. We have to figure out how are we going to make this technology something that better serves the people, the consumers who are buying it."

Risks and concerns

Consumers are turning to internet-connected devices, and while they present enormous opportunities for convenience, they are not without risks.

In prepared testimony before the subcommittee, Robert Mayer, senior vice president for cybersecurity at the United States Telecom Association (USTelecom) said there is "ample evidence of IoT security vulnerabilities," with incidents like cameras being used for spying, personal information being stolen and hackers taking control of devices like smart thermostats.

"Concerns of this kind can have a massive influence on public perception of technologies, and if not addressed in meaningful ways, trust in the digital ecosystem will erode, causing unpredictable levels of disruption and economic harm," Mayer's testimony reads.

There have already been several major hacks of IoT devices, including the Mirai DDoS botnet attack in October 2016 that rocked technology company Dyn and resulted in the dramatic slowing or bringing down of the internet across the East Coast and elsewhere in the world.

In written testimony, Mike Bergman, vice president of technology and standards at the Consumer Technology Association (CTA), warned of the international nature of the attack; 89.1% of the attack traffic originated from devices installed outside the United States, he said.

Read full story here…