ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL

MEMORANDUM

DATE: February 18, 2019

TO: Honorable Jennifer Williamson, Chair
House Judiciary Committee

FROM: Cheryl Hiemstra, Deputy Legislative Director

SUBJECT: House Bill 2395 – Internet of Things

This testimony is presented in support of House Bill 2395

HOUSE BILL 2395:
PROTECT CONSUMERS, PROTECT NATIONAL SECURITY: INTERNET OF THINGS

Background

Currently, everything from toasters to televisions is connected to the Internet, gathering and using a wide range of information. These devices are known as "the Internet of Things," or "smart" devices. Some estimate there will be 25 billion connected devices by 2020. These devices can improve quality of life for many, but these devices are sometimes manufactured without cybersecurity in mind.

The Federal Bureau of Investigation, in a 2018 Public Service Announcement, stated that IOT devices in developed nations are particularly attractive targets.[1] Even now, malicious actors are using compromised devices to buy and sell illegal images and goods, conduct data breaches, send spam, and to act more anonymously. When bad actors can wear the mask of a consumer's IOT device, they are better able to pass through filters and access legitimate business websites for financial exploitation.

Additionally, the National Cybersecurity and Communications Integration Center of the Department of Homeland Security warns about the widespread scale problem of unsecured devices:

> Though many security and resilience risks are not new, the scale of interconnectedness created by the Internet of Things increases the consequences of known risks and creates new ones. Attackers take advantage of this scale to infect large segments of devices at a time, allowing

[1] https://www.ic3.gov/media/2018/180802.aspx

them to access to the data on those devices, or to, as part of a botnet, attack other computers or devices for malicious intent.[2]

The concerns are not hypothetical. When a large network of these devices are compromised, bad actors are able to create a "botnet." In 2016, the Mirai Botnet took shut down nearly the entire eastern United States. Researchers later determined that it infected nearly 65,000 devices in its first 20 hours, doubling in size every 76 minutes, and ultimately built a sustained strength of between 200,000 and 300,000 infections.[3] In the wake of the Botnet, a Chinese company recalled 4.3 million unsecured connected cameras.[4]

On the smaller, but just as important scale, individual consumers with devices that are not built with safety in mind can, unwittingly, be exposing intimate details of their lives to bad actors. Home surveillance, microphone-enabled listening devices, and even kitchen appliances can reveal a lot about a person. When these devices are compromised, the data and information stolen can rise to the same -- or possibly even more -- invasive level than a physical robbery.

Twin concerns of privacy and security should make the reasonable security of these devices a priority.

Concept

House Bill 2395 requires a person that manufactures a device that is sold in Oregon to equip the connected device with reasonable security features. The features should protect information that the connected device collects, contains, stores or transmits from access, destruction modification, use or disclosure that the consumer does not authorize. A failure to build in reasonable security would be a violation of Oregon's consumer protection law enforced by the Attorney General.

The Department of Justice has been coordinating with the technology and other industry stakeholders to work on the best language possible for all Oregonians. A draft version of the current language under consideration is included in the corresponding written testimony.

Contact: Cheryl Hiemstra, Deputy Legislative Director, 971-701-0457, cheryl.hiemstra@doj.state.or.us

[2] https://www.us-cert.gov/ncas/tips/ST17-001
[3] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
[4] https://www.wired.co.uk/article/internet-down-dyn-october-2016