BRIAN E. FROSH
Attorney General

ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

(410) 576-6566 (F)

WRITER'S DIRECT DIAL NO.

(410) 576-6307

February 19, 2020

TO: The Honorable Delores G. Kelley, Chair
Finance Committee

FROM: Steven M. Sakamoto-Wengel
Consumer Protection Counsel for Regulation, Legislation and Policy

RE: Senate Bill 443 – Consumer Protection -- Security Features for Connected Devices (SUPPORT)

The Consumer Protection Division of the Office of the Attorney General supports Senate Bill 433, sponsored by Senators Lee, Patterson and Rosapepe, which would take a meaningful first step in protecting us from unsecured internet-connected devices that are collecting sensitive information about us. The Consumer Protection Division has a long-standing commitment to promoting data security.

Marylanders are welcoming large numbers of connected devices into our lives. We have internet-connected smart speakers, thermostats, refrigerators, televisions, cars, children's toys, and even home security systems with cameras recording inside our homes. Some of that is good – technology should make our lives easier.

However, the security of these devices has lagged behind the innovation. Currently, there are no clear rules governing the security features that manufacturers of these products must include[1] before they place these devices into commerce and into our homes. A large number of these devices have fatally-flawed password protection. Some connected device manufacturers set the same default password for all of their devices, and do not force consumers to change it. For example, imagine 100,000 internet-connected children's dolls being sold, each with a preset password of "12345" or "password." Once that is discovered, either by being easily guessed, or by someone who buys the doll, all 100,000 are accessible. Worse yet, in many other connected devices, these default credentials are hardcoded into the device's firmware. In that situation, a consumer is able to use the device without ever being asked to create or enter a username or password, and the vulnerability can only be fixed by recalling the product.

[1] California and Oregon have passed laws, which are similar to this bill. *See* California Senate Bill 327 Information Privacy: Connected Devices (2017-2018), and Oregon House Bill 2395 (effective January 1, 2020).

The consequences of a connected device getting hacked and controlled can be significant. A vulnerable device can serve as an access point to the rest of a consumer's home network, putting their broader security and physical safety at risk. Certain devices, like medical devices and cars, present the risk of ransomware attacks (e.g., pay us $250 if you want to start your car). Other devices can be targeted for the personal information that they hold, such as children's toys that hold recordings of the children or home alarm systems that track your patterns of activity.

This bill provides useful guidance. It requires manufacturers to equip their devices with a reasonable security feature, and allows them to accomplish that by simply either: (1) giving each device a unique password, or (2) requiring the user to set up their own password before they are able to use the device. Any responsible manufacturer is already complying with this requirement (for example, manufacturers of computers or smart phones will not have to change their practices). Yet because many manufacturers are not, this bill is necessary.

Existing law is inadequate to cover this, as our privacy laws focus on protecting specific categories of information once it has been collected. This bill adds protection to the data-collecting devices prior to their gathering our sensitive personal information. With the wave of these devices being thrust into commerce, this step should be taken now, before more of our data is exposed by unsecured devices.

The Division respectfully requests that the Senate Finance Committee give Senate Bill 433 a favorable report.