HOUSE AMENDMENTS TO
HOUSE BILL 2395
By COMMITTEE ON JUDICIARY
April 11

On page 1 of the printed bill, delete lines 5 through 30.
On page 2, delete lines 1 through 11 and insert:

“SECTION 1. (1) As used in this section:
“(a) ‘Connected device’ means a device or other physical object that:
“(A) Connects, directly or indirectly, to the Internet and is used primarily for personal,
family or household purposes; and
“(B) Is assigned an Internet Protocol address or another address or number that identi-
fies the connected device for the purpose of making a short-range wireless connection to
another device.
“(b) ‘Manufacturer’ means a person that makes a connected device and sells or offers to
sell the connected device in this state.
“(c) ‘Reasonable security features’ means methods to protect a connected device, and any
information the connected device stores, from unauthorized access, destruction, use, modi-
ification or disclosure that are appropriate for the nature and function of the connected de-
vice and for the type of information the connected device may collect, store or transmit.
“(2) A manufacturer shall equip a connected device with reasonable security features. A
reasonable security feature may consist of:
“(a) A means for authentication from outside a local area network, including:
“(A) A preprogrammed password that is unique for each connected device; or
“(B) A requirement that a user generate a new means of authentication before gaining
access to the connected device for the first time; or
“(b) Compliance with requirements of federal law or federal regulations that apply to
security measures for connected devices.
“(3) This section does not:
“(a) Require a provider of an electronic store, gateway, marketplace or other means for
purchasing or downloading software or firmware to verify or enforce compliance with the
provisions of this section.
“(b) Require a person to prevent a consumer from having or obtaining full control over
a connected device, including the ability to modify the connected device or any software or
firmware installed on the connected device.
“(c) Limit the authority of a law enforcement officer or law enforcement agency to ob-
tain information from a manufacturer as provided by law or authorized in an order from a
court of competent jurisdiction.
“(d) Impose a duty on a manufacturer to provide reasonable security features for soft-
ware, firmware or peripheral devices that another manufacturer makes and that a consumer
installs in or adds to the connected device.

“(4) This section does not apply to:

“(a) A connected device on which a consumer installs or otherwise adds software or other devices that the manufacturer of the connected device does not approve for use with the connected device or that damages, evades, disables or otherwise modifies the reasonable security features that a manufacturer incorporates into the connected device.

“(b) A covered entity, a health care provider, a business associate, a health care service plan, a contractor, an employer or another person that is subject to the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, 110 Stat. 1936) or regulations promulgated under the Act, with respect to any action that the Act regulates.

“(c) A connected device, the functions of which are subject to and comply with the requirements, regulations and guidance that the United States Food and Drug Administration promulgates under 21 C.F.R. parts 800 to 1299 or other requirements, regulations and guidance the United States Food and Drug Administration promulgates with respect to medical devices, including software as a medical device.

“(5) The duties and obligations that this section imposes are in addition to and not in lieu of any other duties and obligations imposed under other applicable law and do not relieve any person from the person's duties and obligations under any other applicable law.

“(6) A manufacturer that violates subsection (2) of this section engages in an unlawful trade practice under ORS 646.607.”