DEBBIE DINGELL
12TH DISTRICT, MICHIGAN

116 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4071

HOUSE COMMITTEE ON
ENERGY AND COMMERCE
SUBCOMMITTEES ON
HEALTH
ENVIRONMENT AND CLIMATE CHANGE
COMMUNICATIONS AND TECHNOLOGY
CONSUMER PROTECTION AND COMMERCE

HOUSE COMMITTEE ON
NATURAL RESOURCES
SUBCOMMITTEES ON
NATIONAL PARKS, FORESTS AND PUBLIC LANDS
OVERSIGHT AND INVESTIGATIONS

Congress of the United States
House of Representatives
Washington, DC 20515

DISTRICT OFFICES:

19855 WEST OUTER DRIVE
SUITE 103-E
DEARBORN, MI 48124
(313) 278-2936

301 WEST MICHIGAN AVENUE
SUITE 400
YPSILANTI, MI 48197
(734) 481-1100

WEBSITE: DEBBIEDINGELL.HOUSE.GOV

October 24, 2019

Mr. Jeff Bezos
Amazon
PO Box 81226
Seattle, WA 98108-1226

Mr. Sundar Pichai
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai and Bezos

Recently a number of articles were published regarding research done by a German cybersecurity company SRLabs in which researchers created apps designed for smart speakers that passed both Google and Amazon security-vetting processes and allowed the app to eavesdrop on users as well as phish for their passwords. While these apps were created and used only for research purposes, there is potential for either copycat apps or that malicious actors have already used these techniques to target consumers and their personal information.

These smart speakers and the advancement of speech recognition technology represent an incredible convenience for consumers, allowing them to bypass screens and for those with physical disabilities to access the internet like everyone else. But the same feature that contributes to that convince, not having a screen, also eliminates an important feedback loop for consumers to understand how these applications are performing and puts your company in an even greater position to look after consumers well-being.

Further, with this added convenience come obvious privacy tradeoffs and as the adoption of smart in-home speakers increases, the incentive for bad actors to manipulate and attack these devices rises as well. Given the rapidly increasing use of this technology it is imperative that consumers know applications running on these speakers are safe and are performing as intended. With that I ask the following questions

- How are you addressing apps like this from being able to obtain this information in the future?
- When will these changes take effect?
- Have you reviewed other applications to see if they attempted similar collection of personal information? If not, will you commit to doing so?
- Is there any evidence other applications have used these techniques to take user audio recordings?
- If there was potential wrongdoing, will users be notified?

- Are you reviewing other "skills" to see if they were used to eavesdrop on consumers?

Thank you for taking the time to review these questions, and I would appreciate your response before November 18. If you or your staff have any questions please feel free to contact Kevin Dollhopf in my office at kevin.dollhopf@mail.house.gov or at (202)225-4071.

Sincerely,

Debbie Dingell

Debbie Dingell
Member of Congress