# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225–5074 MINORITY (202) 225–5051 http://oversight.house.gov

### Opening Statement Ranking Member Robin Kelly

#### Hearing on "Game Changers: Artificial Intelligence Part III, Artificial Intelligence and Public Policy" Subcommittee on Information Technology

#### April 18, 2018

Thank you Chairman Hurd, and welcome to all of our witnesses here today.

This is the third hearing our Subcommittee has held on the important topic of artificial intelligence or AI. Our two prior hearings have shown how critical the collection of data is to the development and expansion of AI. However, AI's reliance on the use of personal information raises legitimate concerns about personal privacy.

Smart devices of all kinds are collecting your data. Many of us have to look no further than the smart watch on our wrist to see this evidence in motion. The arms race to produce individual predictive results is only increasing with smart assistants like Alexa and Siri in your pocket and listening at home for your next command. Sophisticated algorithms help these machines refine their suggestions and place the most relevant information in front of customers. These systems, however, rely upon vast amounts of data to produce precise results.

Privacy concerns for tens of millions of Facebook users were triggered when the public learned that Cambridge Analytica improperly obtained and potentially used their personal data to promote the candidacy of Donald Trump.

Whether Congress passes new laws or industry adopts new practices, clearly consumers need and deserve new protections.

To help us understand what some of those protections may look like, Dr. Ben Buchanan from Harvard University's Belfer Center for Science and International Affairs, is here with us today. Dr. Buchanan has written extensively on the different types of safeguards that may be deployed on AI systems to protect the personal data of consumers.

Advancements in AI also pose new challenges to cybersecurity due to increased risks of data breaches by sophisticated hackers. Since 2013, we have witnessed a steady increase in the number of devastating cyberattacks against both the private and public sectors. This past September, Equifax announced that hackers were able to exploit a vulnerability on their systems, and as a result, gained access to the personal data of over 140 million Americans. A recent report co-authored by OpenAI, represented by Mr. Clark today, expressly warns about the increased cyber risks the country faces due to AI's advancement. According to the report, continuing AI advancements are likely to result in cyberattacks that are "more effective, more finely targeted, more difficult to attribute, and more likely to exploit vulnerabilities in AI systems."

As AI advances, another critical concern is its potential impact on employment. Last year, the McKinsey Global Institute released the findings from its study on the potential impact of AI-driven automation on jobs. According to the report, "up to 1/3 of [the] workforce in the United States and Germany may need to find work in new occupations." Other studies indicate that the impact on U.S. workers may even be higher. In 2013, Oxford University reported on a study that found that due to AI automation, "about 47 percent of total U.S. employment is at risk."

To ensure that AI's economic benefits are more broadly shared by U.S. workers, Congress should begin to examine and develop policies and legislation that would assist workers whose jobs may be adversely affected by AI-driven automation.

As AI advances continue to develop, I'll be focused on how the private sector, Congress, and regulators can work to ensure that consumers' personal privacy is adequately protected, and that more is being done to account for the technology's impact on cybersecurity, and our economy. I want to thank our witnesses for testifying today, and I look forward to hearing your thoughts on how we can achieve this goal.

Thank you again, Mr. Chairman. I yield back.

Contact: Aryele Bradford, Deputy Communications Director, (202) 225-1782.