After Facebook Privacy Scandal, Capitol Hill Turns Eye to Privacy Matters

In terms of companies protecting citizen data, we have a long ways to go.

Amanda Ziadeh

Thu, 04/19/2018 - 12:13

Illustration: uzenzen/iStock

In the final installment of the House IT subcommittee's three-part hearing series on artificial intelligence, two particular topics were discussed more than before: the privacy of citizen data and the importance of measuring AI capabilities.

The hearings began in February with industry experts suggesting the U.S. invest more in AI research. At the Subcommittee on Information Technology's second hearing in March, government officials testified about their agency current use of and funds for AI and AI research amid recent budget proposals.

The last hearing on April 18 welcomed AI experts from nonprofits and academia, and the conversation went beyond investments and fundings to the AI responsibilities of both government and industry.

So, considering the Facebook-Cambridge Analytica affair and recent data breaches, Rep. Robin Kelly, D-Illinois, had questions about AI systems' use of personal data and how to preserve citizen privacy.

The consensus? In terms of companies protecting citizen data, we have a long ways to go. In his testimony, Ben Buchanan, a postdoctoral fellow at the Science, Technology, and Public Policy Program at Harvard Kennedy School's Belfer Center for Science and International Affairs, provided technical approaches that can mitigate this problem.

Privacy

Technology can't replace policy, but innovations like differential privacy can ensure a particular individual's data is obscured while retaining a data set's value. This works by adding "statistical noise" to a particular person's data, but the validity of data in the aggregate remains, according to Buchanan.

Another tactic is on-device processing, which brings the AI system to the user, rather than bringing the user's data to an AI system central repository.

These are recent positive technical developments that need more research but are very promising and too infrequently deployed. So, why aren't companies using these strategies?

As a matter of practice, "they require enormous technical skill to implement," Buchanan said. "I think some companies want to have the data, want to aggregate the data and see the data, and that's part of their business model."

There's also an "enormous demand" for people with the technical skills required to build and secure these systems, and that demand hasn't yet been met.

When asked how Congress can encourage AI companies to use and adopt more stringent safeguards for protecting consumer personal data, Buchanan referred to fellow panelist and director at OpenAI Jack Clark's remarks on the importance on

measurement.

“This is an area that I would like to know more about and measure better. How are American companies storing, securing and processing the data on Americans?” Buchanan said. Considering measurement is a topic of interest to the subcommittee, as its chairman, Rep. Will Hurd, R-Texas, mentioned, Buchanan said this would be a good place to start.

Measurement

“We must measure the progress and capabilities of AI to guide effective policymaking,” Clark said.

The use of AI in cyber will lead to more effective and targeted cyberattacks, and will more likely exploit vulnerabilities in AI systems.

“You can think of AI as something that we’re going to add to pretty much ever aspect of technology,” Clark said, adding power and capabilities.

Doing so will make U.S. defenses better, but Clark said it’s not clear yet whether this favors the defender or the attacker, and that’s where competitions come in.

“Hosting competitions, having government measure these capabilities as they develop will give us a kind of early warning system,” Clark said. If something bad is going to happen as a consequence of an AI capability, the government should know about it beforehand.

“I’d like an organization or an agency to be telling us about that,” Clark added. This is an opportunity to learn in an unprecedented way about the future before it happens, in order to make the appropriate regulations before harm occurs.

Clark refers to competitions like the Defense Advanced Research Projects Agency’s Cyber Grand Challenge initiative in 2016 to create advanced, automatic defensive systems, and the Defense Innovation Unit Experimental xView Detection Challenge (and data release) to develop new solutions for national security and disaster response.

Challenges like these, especially in the realm of robot manufacturing, drone navigation and predictability of AI systems, can “catalyze progress which would

lead to commercial innovations and an increase in the robustness and usability of the technology," Clark said.

He recommend the U.S. fund and encourage agencies to host more competitions in these areas, because a multitude of governmentwide competitions can spur innovation and AI predictions. Every agency has its focus areas and awareness of threats and challenges the private sector does not.

Hurd said the subcommittee will release a summary of what it has learned from this AI hearing series in the coming weeks, outlining steps that should be taken to responsibly help drive AI.

View printer friendly version
Will Hurd
AI
capitol hill
data
privacy
Eye on AI
DIUx
Non-feature