Adam I. Klein
Director, Robert Strauss Center on International Security and Law
University of Texas at Austin

Response to Senator Klobuchar Questions for the Record:

Privacy, Technology, and the Law Subcommittee of the Judiciary Committee hearing on "Protecting Americans' Private Information from Hostile Foreign Powers"

Questions for Adam Klein, former Chair of the Privacy and Civil Liberties Oversight Board

Connected devices—from thermostats and speakers to vacuum cleaners—raise serious privacy concerns. Many of these smart devices continuously collect and store voice data in people's homes, and may also share sensitive data with third-party developers.

- How vulnerable are these connected devices, and the systems where the data they collect is stored, to hackers?

Official analyses and news reports have repeatedly identified poor security practices in internet-connected devices, enabling them to be hijacked for botnets and other malicious activity. For example, the Mirai botnet harnessed a vast army of internet-connected cameras and other devices using insecure default passwords.

As the Cybersecurity Solarium Commission explained, the advent of 5G networks will

> **dramatically increase the "attack surface," or the exposed routes through which malicious actors can threaten our networks. An exponential increase in connected devices will more deeply embed the internet in our lives and may, in turn, lead to a rise in the everyday leakage of private data. Worse still, security vulnerabilities will spread into sectors not traditionally associated with cyberspace (e.g., transportation, agriculture, or health care) and thereby increase the risk of catastrophic systemic failures.**

Internet of Things devices are also a potential source of data-leakage to hostile foreign powers. As the researcher Aynne Kokas has noted, some Chinese-built Internet of Things devices transfer the data they collect to servers in China. These products may record intimate details about what takes place in the home, on corporate networks, and in other sensitive locations. That data may then be available to China's intelligence services, which can use it to harm Americans in various ways.

- What measures are necessary to help ensure consumers' data privacy is protected when it comes to products like these?

Leakage of sensitive IoT data to hostile foreign powers is a matter of national security concern. Hostile intelligence services can use this information to target Americans for recruitment, to inform transnational repression of dissidents and other regime opponents, to fuel influence campaigns, or to refine social-engineering and phishing attacks.

Congress and the Executive Branch should curtail IoT data-handling practices that endanger national security in this way. For example, IoT devices should be prohibited from storing certain categories of especially sensitive data on servers located in the PRC or that can be accessed by PRC entities.