United States Senate
WASHINGTON, DC 20510–3703

May 15, 2017

Dr. Katharine G. Abraham
Chairperson
Commission on Evidence-Based Policymaking
University of Maryland

Dr. Ron Haskins
Co-Chairperson
Commission on Evidence-Based Policymaking
Brookings Institution

Dear Dr. Abraham, Dr. Haskins, and members of the Commission on Evidence-Based Policymaking:

As the Commission on Evidence-Based Policymaking works to finalize its conclusions and recommendations to Congress, I write to remind the commission that new government databases, even if they are created for well-intended purposes, can both threaten the liberty of Americans and create an irresistible target for criminal hackers and foreign governments. For that reason, I strongly urge the commission to recommend that privacy enhancing technologies (PETs), such as secure multi-party computation (MPC) and differential privacy, must be utilized by agencies and organizations that seek to draw public policy related insights from the private data of Americans.

As the commission's website states, "[t]he Commission on Evidence-Based Policymaking (CEP) was established to develop a strategy for increasing the availability and use of data in order to build evidence about government programs, while protecting privacy and confidentiality." I am particularly interested in the commission's strategic efforts to protect the security and confidentiality of the underlying data sources. Sensitive information on American citizens is, in many cases necessarily, collected and stored in public and private sector databases across the globe. Daily news stories highlighting the vulnerability of such databases to breaches, cyberattacks, and mass hacking demonstrate that those charged with securing sensitive data often fail to use best practices or advanced technology to protect the data. This only reinforces the importance of this aspect of the commission's mission.

Any efforts to collect, store, or utilize data for the laudable goal of improving government programs must also protect Americans' personal, sensitive data. It is my belief that these goals need not be at odds. As you heard during testimony at the commission's sixth meeting on February 24, 2017, advancements in the field of secure multi-party computation and differential

privacy can enable researchers to answer key policy questions without the creation of new, sensitive databases or data linkages. Secure MPC practices allow two or more parties to perform computations simultaneously with merged encrypted data, thereby protecting each initial data set. For years, U.S. taxpayer funds have supported research into secure MPC, differential privacy, and other PETs. These technologies are being utilized in other countries and the private sector, enabling researchers to gain useful insights from data without creating new databases that could be lost, stolen or seized by the authorities. I believe it is time for the U.S. public sector to implement such practices and bring them to scale.

I am hopeful that the commission's recommendations will lay a roadmap for developing executive and legislative branch strategies to advance the use of evidence in policymaking. Given the current global and domestic climate, the importance of sound recommendations related to data security cannot be overstated and a failure to adequately address these issues could undermine the good and thorough work the commission has undertaken over the past year. Accordingly, it is my hope that the commission embraces moving beyond a bare legal framework to protect individual private data and recommend requiring technological solutions such as secure multi-party computation and differential privacy in particular.

Sincerely,

Ron Wyden
U.S. Senator