The Secure Research Data Network Act

The Federal government holds vast amounts of useful data that could improve Americans' lives by answering pressing policy questions, from understanding the gaps in veteran's access to SNAP and WIC programs, to using data on education and employment to better target federal workforce development and assistance programs. Unfortunately, data held by government agencies is siloed, blocking research that could support smart, evidence-based policymaking. In its 2017 report, the U.S. Commission on Evidence-Based Policymaking reported that 87% of agencies surveyed had difficulty accessing the data they need, as it is often held by other agencies or in a form that cannot be easily analyzed. In response to this concern, the Commission recommended the creation of pilots to create secure ways to share data between agencies. This bill would create a Secure Research Data Network to do just that.

At the same time, a centralized data asset containing reams of linked inter-agency data is an attractive target for hackers and foreign adversaries. To facilitate legitimate data use while minimizing cyber risk, this bill requires the use of zero-trust encryption technology like Secure Multiparty Computation (SMPC), which allow approved researchers to calculate statistics based on encrypted data while protecting the raw data from theft or abuse. Experts agree that SMPC technology, which was developed with support from the National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA), is the best tool for this kind of task — for example, the Boston Women's Workforce Council has used SMPC for the past six years to study the gender wage gap by analyzing 250+ employers' wage data, without that data ever needing to leave each company's servers. By requiring the use of privacy-enhancing technology, the Secure Research Data Network Act would let Americans benefit from smart, evidence-based policy decisions without compromising their privacy.

The Secure Research Data Network Act would:

- Authorize $100 million for a 3-year pilot (which can be extended by 2 years) of a Secure Research Data Network (SRDN).
- Require SRDN, which will be housed in NSF, to develop, distribute, and run a free, open-source software data platform to provide approved researchers with secure access to government-held data without risking Americans' privacy and security.
- Require the use of Secure Multi-Party Computation or other equivalent privacy techniques to protect the data used for SRDN projects.
- Establish data quality service and training teams in the SRDN, which will, at no cost to agencies, help agencies to prepare their data and facilitate agency participation.
- Establish an SRDN advisory board, which will evaluate proposed research projects, with input from the public, before providing researchers access to the SRDN platform.
- Require GAO to evaluate the SRDN pilot at its conclusion and the potential use of the SRDN platform to address other government needs.

Endorsements: Data Coalition, Consortium of Social Science Associations, Bipartisan Policy Research Center, MPC Alliance, Demand Progress, Institute for Veterans and Military Families, Student Veterans for America, Axciom, Bosch, Dr. Mayank Varia (Boston University), Dr. Amy O'Hara (Georgetown Massive Data Institute), Dr. Rafail Ostrovsky (University of California Los Angeles), Dr. Seny Kamara (Brown University), Dr. Nigel Smart (University of Leuven, Belgium), Dr. Jonathan Katz (University of Maryland).