epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

September 25, 2017

The Honorable Trey Gowdy, Chairman
The Honorable Elijah Cummings, Ranking Member
U.S. House Committee on Oversight & Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Gowdy and Ranking Member Cummings:

We write to you regarding the upcoming hearing "Recommendations of the Commission on Evidence Based Policymaking."[1] The Electronic Privacy Information Center ("EPIC") strongly supports the efforts of the Commission to make data in the federal government more widely available to ensure better policymaking. At the same time, where data maintained by the federal government implicates identifiable individuals, privacy risks must be addressed and reduced as much as possible.

EPIC was founded in 1994 to focus attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has long advocated for privacy and security safeguards for data as well as the use of privacy enhancing technologies ("PETs") that minimize or eliminate the collection of personally identifiable information.[2] EPIC testified before the Commission last year and called for the Commission to adopt innovative privacy safeguards to protect personal data and make informed public policy decisions.[3] Additionally, EPIC President Marc Rotenberg and EPIC Advisory Board member Cynthia Dwork served on a panel at the National Academies of Science that recently released a report on how federal data sources can be used for public policy research while protecting privacy.[4]

[1] *Recommendations of the Commission on Evidence-Based Policymaking*, 115th Cong. (2017), H. Comm. on Oversight & Government Reform, https://oversight.house.gov/hearing/recommendations-commission-evidence-based-policymaking/.

[2] EPIC Executive Director Marc Rotenberg, Testimony Before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Mar. 1, 2001, *Privacy in the Commercial World,*

[3] Marc Rotenberg, *Commission on Evidence-Based Policymaking: Privacy Perspectives,* before the National Academies of Science, Sep. 9, 2016, https://epic.org/privacy/wiretap/Rotenberg-CEBP-9-16.pdf.

[4] National Academies of Science, "Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy" (2017), https://www.nap.edu/catalog/24652/innovations-in-federal-statistics-combining-data-sources-while-protecting-privacy [hereinafter "Innovations in Federal Statistics"].

EPIC endorses several of the Commission's recommendations. Requiring comprehensive risk assessments for de-identified confidential data and supporting adoption of PETs are key recommendations of the Commission's report that will serve to protect personal information. Even where data has been de-identified it is still possible to combine certain data sets with others to determine extensive amounts of personal information.[5] Moving forward, this Committee and Congress should heed the calls of the Commission for the adoption of PETs to reduce the risk of re-identification of personal data. As was noted in the report by the National Academies of Science:

> Any consideration of expanding data must have privacy as a core value…As federal agencies seek to combine multiple datasets, they need to simultaneously address how to control risks from privacy breaches. Privacy-enhancing techniques and privacy-preserving statistical data analysis can be valuable in these efforts and enable the use of private-sector and other alternative data sources for federal statistics.[6]

Equally important is to recognize that under the Privacy Act statistical data is subject to fewer privacy constraints because it is understood that statistical does not identify specific individuals. If it is possible to re-identify aggregate data, complete privacy protections must necessarily apply. Agencies will carry the responsibility to ensure the adequacy of the privacy enhancing and privacy protecting techniques.

It is necessary to note that there need not be any tradeoffs between evidence based policy and privacy protections. Many government data sets do not implicate privacy protections at all.[7] Meteorological data, for example, has become increasingly important as the severity of storms has increased. The government should make this information widely available to the public to improve emergency planning and promote public safety.

The Commission also proposes a National Secure Data Service ("NSDS") to facilitate data access for the purposes of evidence building. Establishing an entity that helps analyze data from multiple sources should help ensure that data sets can be combined and used securely in a defined set of circumstances. At the same time, there are real challenges to ensure that the creation of the NSDS does not create a centralized repository of data on Americans, like the proposed National Data Center which was broadly opposed by the public and led to the enactment of the Privacy Act.

We ask that this letter from EPIC be entered in the hearing record.

[5] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Melon University, Data Privacy Working Paper, 2000, https://dataprivacylab.org/projects/identifiability/paper1.pdf

[6] Innovations in Federal Statistics at 3.

[7] *See e.g.* National Hurricane Center, *NHD Data Archive,* http://www.nhc.noaa.gov/data/.

EPIC looks forward to working with the Committee to promote the use of government enable well informed policies and ensure that necessary privacy techniques are deployed to safeguard personally identifiable information.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow