

**Commission on Evidence-Based Policymaking:**

**September 9, 2016**

**Open Meeting**

**Commissioners Present:**

Katharine G. Abraham, Chair  
Ron Haskins, Co-Chair  
Sherry Glied  
Robert Groves  
Robert W. Hahn  
Hilary Hoynes  
Jeffrey Liebman  
Bruce D. Meyer  
Paul Ohm  
Allison B. Orris  
Kathleen Rice  
Latanya Sweeney  
Kenneth Troske  
Kim Wallin

The open meeting was called to order at 1:00 PM. Chair Katharine Abraham provided an introduction.

**Panel 1: Overview of Federal Approaches to Privacy**

*Marc Groman, OMB:*

*(accompanied by Christa Jones, Census, Privacy Council member.)*

- Privacy is about people.
- Privacy is not a roadblock for us, but a fundamental for long-term success. Privacy encourages innovation and the adaption of new technology.
- OMB Circular A-130 outlines privacy as a continuous and risk-based concept, not just something that can be checked off for legal compliance. We must consider that we are not eliminating risk and acknowledge residual risk, and be accountable for the risk.
- Make use of de-identification based on current technology
- Recommended developing privacy talent by improving hiring practices and training for the current workforce.
- Federal privacy and statistical communities are joining forces because they have a common goal

*Katherine Wallman, Chief Statistician of the United States, OMB:*

- CIPSEA is a strong confidentiality law designed for statistical and other agencies to protect data acquired for exclusively statistical purposes.

- CIPSEA took a long time to become law, despite widespread agreement within the Administration, and support in the Congress. In fact, there is still a piece of "unfinished business" with the so-called "tax companion" bill.
- CIPSEA implementation guidance includes policies to minimize risk of disclosure and provide severe penalties for disclosure.
- Procedures to minimize risk in implementing CIPSEA include staff training, physical and information systems security, disclosure review.

*Discussion and Questions:*

- Commissioner Ohm asked about notice and consent. Mr. Groman answered that there is still a role for the FIPPS, including notice and consent, and there are limitations that we need to grapple with. He sees the FIPPS as dials, i.e., if one is difficult to implement one could dial up others. He sees a role for privacy principles tailored for specific initiatives. He gave the example of the President's Precision Medicine Initiative (PMI), which uses a model of individual participation rather than open-ended consent.
- Commissioner Rice asked about compliance for PMI. Mr. Groman described that it is a very new initiative.
- Commissioner Rice asked about notice and consent for data collection. Mr. Groman clarified that transparency is an important feature of the Privacy Act and it is important to notify respondents about privacy risks and benefits.
- Commissioner Groves asked if the Clearinghouse was solely for statistical use, would CIPSEA cover it? Mr. Groman declined to respond. Ms. Christa Jones said that the source agency Privacy Act System or Records Notices (SORNs) for each dataset added to the clearinghouse would need to be revised before transferring data to the clearinghouse. And she suggested that CIPSEA would cover data in the Clearinghouse as happens, by way of analogy, to administrative data acquired by the Census Bureau, which gain Title 13 confidentiality protections.
- Commissioner Troske asked both speakers how a clearinghouse could lower risks. Mr. Groman said having all the data centralized could streamline the process of access. Ms. Wallman said that Research Data Centers can provide an example for how to create a clearinghouse.
- Mr. Groman advised that the Commission consider different cultural perceptions of privacy.
- Commissioner Meyer asked what gaps need to be addressed in the law. Mr. Groman indicated updating A-130 recently helped clarify privacy regulations.

**Panel 2: State Legal Perspectives**

***Amy Guidera: Data Quality Campaign; Building Trust is Critical to an Evidence-Based Culture: Lessons from the Education Sector***

- People won't use the data unless it's both valuable and trustworthy. Indicated that "privacy is not a compliance exercise."

- "There are four different federal laws that prohibit" the federal government from accessing student data, or creating a national student-unit record system. Ms. Guidera's recommendations for the Commission:
  - Measure what matters: be clear about what you want to achieve. For example, federal reviews of data collections and sunsets for unnecessary collections may be merited.
  - Break down federal data silos, get federal data house in order and better align data across agencies.
  - Be Transparent-- promote timely public indicators based on stakeholder questions, promote greater federal transparency. Link state data systems.
  - Guarantee access and protect privacy- build capacity to use data effectively, provide incentives for states and districts

***Justin Erlich: Open Justice***

- Mr. Erlich described what he characterized as tension between transparency and privacy.
- California developed an Open data portal to make statistics available to the public related to justice. Unique issues emerged regarding justice data. Mr. Erlich cited an example of a firm posting booking photos available through public records on a website, and charging individuals to remove those photos.
- Mr. Erlich described the presence of "linkage attacks," incidents where in smaller communities individuals in administrative datasets can be identified through press reports. Mr. Erlich described that restrictions in place for FERPA and HIPPA are not present in the law enforcement community.
- California utilizes tiered access to promote "responsible transparency." The tiers include public release, researcher only release, and internal use only (i.e., researchers come into the enclave).
- Mr. Erlich described "dataset snowflakes," where each dataset is different, and that states are looking for additional guidance on how to think about privacy risk.

***Michael Basil: State Legal Perspectives from Illinois***

- Mr. Basil indicated that states need to focus on calibrating an approach to managing data while protecting privacy.
- Mr. Basil described challenges within Illinois in interpreting access to some administrative datasets. For example, Mr. Basil cited that universities' access to unemployment insurance data to evaluate program effectiveness and career readiness varies under the law, depending on whether they are public or private institutions.
- One strategy for providing access within Illinois in an effort to be safe and transparent, was the development of an enterprise Memorandum of Understanding (eMOU) between state agencies.
- The eMOU provides a standardized process for agencies as a way to improve coordination. Mr. Basil indicated the state is considering an external eMOU, and that such an agreement could be used with common standards across federal agencies.

### *Discussion and questions:*

- Commissioner Wallin asked Mr. Basil if individuals have to go to each agency separately to request data through the eMOU. Mr. Basil indicated the process is established for sending a form to each agency, similar to a FOIA but enables quick requests electronically.
- Commissioner Troske asked if the eMOU can be renewed or whether individuals need to request each time? Mr. Basil responded that currently individuals do need to request each time, but duration is included in the initial request.
- Commissioner Groves asked: What is the incentive to agencies to share their data through their eMOU? Mr. Basil responded that the eMOU streamlines the process for both parties, and there are also consequences for not complying. Mr. Basil also suggested that the executive branch in the state can influence agency participation. Chair Abraham asked if data will be made available to outside researchers. Mr. Basil responded that the system is not currently equipped for external access, but the success of the current system could build on it. The administration in Illinois also supports using the data for research.
- Co-Chair Haskins asked about how to persuade Congress to allow more access to education data, considering the issues around FERPA. Ms. Guidera said that the Commission will allow for some discussion of this outside of the pressure of creating legislation, and may lead to better education data access.

15 minute break at 3:00 PM.

### **Panel 3: Other Privacy Perspectives**

- ***Marc Rotenberg, Electronic Privacy Information Center (EPIC): Commission on Evidence-Based Policymaking-Privacy Perspectives*** Mr. Rotenberg described a case study of Federal Wiretap Reports to encourage that the Commission not think about balancing privacy against access, but rather to think about access while providing for privacy protections.
- One key consideration is the notion of PII, which is a core concept in modern privacy law. Goal is to ensure fairness, accuracy, accountability.
  - The boundaries of PII have been increasingly “permeable.” If entities can establish the ability to recreate or re-identify, then those entities have obligations to protect privacy. The burden is on organizations to establish that available techniques can achieve privacy goals.
- Identity theft is a top concern of consumers. Data are increasingly under attack from malicious actors. Even well intentioned data collection may end badly.
- There are hard problems ahead to address: (1) data are dynamic posing challenges in assessing risks, (2) data are increasingly under attack from malicious interests, and (3) a recent emphasis on big data raises new questions
- Mr. Rotenberg indicated there is a need to anticipate new uses, not just present uses of data. He said “Data is the basis of research, innovation, economic growth, and informed policy decisions. Data are also the basis for profiling, tracking, segmentation, and discrimination. Privacy protections for data are necessary to maximize the benefits and minimize the risks.”

***Cynthia Dwork (via videoconference): Microsoft, Differential Privacy and its Properties***

- Dr. Dwork suggested that formal privacy guarantees are needed in government.
- A Fundamental Law of Information Recovery suggests that accuracy in estimates from multiple statistics can reduce privacy, and the law cannot be circumvented
- Differential privacy is a mathematical procedure that enables individuals' data to be used in a range of studies and analyses by measuring "privacy loss"
- Dr. Dwork provided three recommendations to the Commission in considering applications of differential privacy:
  - Publish your epsilon, the identified cap on privacy loss. Disclosure of these estimates could lower privacy costs, and encourage improvements in a manner similar to the EPA's Toxics Release Inventory disclosure system.
  - Establish a list of approved private data analysis techniques and keep it current.
  - Consider restraint, if needed. Sometimes the costs may be too much in balancing the need for statistics and privacy.

*Discussion and Questions:*

- Commissioner Ohm asked if differential privacy is the most superior technique. If the Commission were to recommend differential privacy and nothing else, would it be a solution? Dr. Dwork answered that you should try to be differentially private, but if not possible, explain why. Dr. Dwork encouraged that entities explain why individual observations are needed, or what is lost if they are omitted.
- Commissioner Hahn asked if the presumption is that everyone plays by the rules in implementing differential privacy. Dr. Dwork responded that there has to be a "good guy" somewhere in the picture.
- Commissioner Ohm also asked about the lessons learned from the National Data Center proposal of the 1960s. Mr. Rotenberg responded that the Privacy Act emerged to keep the data in separate repositories and to create restrictions on sharing that increased confidence in data at that time. Today, the risks are still present, but new technologies and innovation now exist.
- Commissioner Hahn noted that a national data center would necessitate a high level of collaboration among agencies that we may not yet have.
- Commissioner Troske said there are examples of national statistical agencies working in northern Europe and asked the speakers about differences with the U.S. Mr. Rotenberg responded that much work has been conducted by the OECD on this, and that one key difference is that the EU has a robust framework for protections. Dr. Dwork responded that some element of control can be captured through the definition of privacy utilized.
- Commissioner Groves stated there is a statistical computing change that needs to happen to design a suite of privacy tools. He recommended staff circulate the transcript of John Abowd's talk about this to the Commission.
- Commissioner Hoynes asked about looking into tiered access privacy models

- Commissioner Ohm asked about the best way to work with the privacy community during the Commission's work. Mr. Rotenberg stated that privacy is an important value in the US, and legal considerations are important. There doesn't have to be a necessary trade-off.

### **Facilitated Discussion**

Commissioner Hahn summarized key questions raised for the Commission to consider throughout the discussion:

- How do we consider data access in a world of non-zero risk, recognizing that all data aren't equal in terms of sensitivity?
- How should policymakers weigh this risk-benefit balance?
- How much better can we be doing than we are doing now? What is the potential of vehicles like the enterprise MOU to address the issues we're faced with?
- What would realistic solutions look like?
- How would we measure and evaluate the likely efficacy of our recommendations?

Commissioner Groves provided summary remarks. Commissioner Groves indicated that the afternoon provided a "sobering reminder" about the need to shift the focus to talking about the advantages of new developments in technology that can enhance privacy protections. Commissioner Groves indicated that the risk of harm is not static over multiple dimensions, including time and populations; what is risky today, may not be risky tomorrow. Commissioner Groves described that in a diverse society, the Commission must be sensitive in its work to cultural considerations in addressing questions raised. The key question to be considered moving forward: can we build a safe environment while also permitting evaluation of government performance? He can't imagine a better time to address these challenges given the growing number of sophisticated data users and the innovations that can improve privacy protections.

Chair Abraham **adjourned** the meeting at 4:22 PM.