Bridging the Gap between Computer Science and Legal Approaches to Privacy

---

Kobbi Nissim (Ben-Gurion University and Harvard University)

Tools satisfying differential privacy are making significant strides towards practical use. For these tools to be applied on sensitive personal information, it is important to demonstrate that they satisfy relevant legal privacy protection requirements. Making such an argument is challenging due to the many conceptual gaps between the legal and technical approaches to defining privacy.

We will articulate some of the gaps between differential privacy and legal approaches to defining privacy and present an argument that differential privacy satisfies the requirements of a particular law - the Family Educational Rights and Privacy Act (FERPA) of 1974. To make this argument, we extract a formal mathematical requirement of privacy based on FERPA and complement it with a proof that differential privacy satisfies the requirements of this model. To handle ambiguities that can lead to different interpretations of the legal standard, we take a conservative "worst-case" approach and attempt to extract a requirement that is robust to potential ambiguities. Hence, our proof demonstrates that differential privacy satisfies a broad range of reasonable interpretations of FERPA.

We will also discuss the generality of our methodology and how it can apply to legal standards other than FERPA.

Joint work with Aaron Bembenek, Mark Bun, Marco Gaboardi, and Salil Vadhan from the Center for Research on Computation and Society, and Urs Gasser, David O'Brien, and Alexandra Wood from the Berkman Center for Internet & Society.