

|  |  |
| --- | --- |
| Differential Privacy: Protecting Individuals from Re-Identification | |
| C:\Users\JBD\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\WTPW0Q86\me2.jpg  Dan Kifer  Vishesh Karwa  Vishesh Karwa  Aleksandra Slavkovic  Aleksandra Slavkovic | A FREE webinar featuring:  **Daniel Kifer, Pennsylvania State University**  **Vishesh Karwa, Harvard University**  Moderator  **Aleksandra Slavkovic, Pennsylvania State University**  Friday, February 10, 2017, 1:00-2:00 p.m. EST  Twitter Hashtag: #ASAwebinar  Sponsored by the **ASA-Privacy & Confidentiality Committee**  Differential privacy is a statistical framework for protecting privacy interests in statistical databases by focusing on the disclosure risk to an individual being included in a data set. In this webinar, two research experts explain this methodology and how they apply differential privacy methodology as a data protection method for protecting data files from the risk of re-identification. A key benefit of the Differential Privacy methodology is that in many cases, appropriate privacy protection *can* be achieved if random noise is properly added to the actual results. For example, rather than simply reporting the sum, the data provider can inject noise based on a distribution. The calculation of “how much” noise to inject can be made based only on knowledge of the function to be computed. This webinar will cover the basic principles of differential privacy, how it works, and how it can successfully be applied to current statistical databases.  *Kifer is currently on sabbatical at the U.S. Census Bureau investigating applications of differential privacy to official statistics. Karwa is currently working on combining statistical and cryptographic approaches for data privacy while privacy preserving statistical inference.* |

**Registration**: This webinar is free, but registration is required:

<https://www.amstat.org/ASA/Education/Web-Based-Lectures.aspx>.