Journal of Privacy and Confidentiality (2010) **2**, Number 1, pp. 1

Editorial: In This Issue

Stephen E. Fienberg*

In this issue of the *Journal of Privacy and Confidentiality*, we continue our focus on the technical aspects of research methodologies and activities in the areas of privacy, confidentiality, and disclosure limitation through a trio of articles, but we begin by reproducing related materials from some other sources on broader aspects of the topics.

Social networking sites on the Internet have recently been much in the news in connection to the issue of access to members' personal information. In particular, earlier this year the largest networking site, *Facebook*, which is approaching 500 million members worldwide, changed how it dealt with privacy settings on individual information spawning a public outcry of major proportions. In a short piece, Bruce Schneier reminds us why claims that "privacy is dead in the age of the Internet" are much exaggerated. We hope to include a more detailed look at the current and past *Facebook* controversies in a future issue of the *Journal*.

Two recent National Research Council reports address the issue of privacy in a broad context and in the specific context of information systems and datamining to counter terrorism. We are especially pleased to reproduce materials from *Engaging Privacy and Information Technology in a Digital Age* (2007) and *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (2008). These excerpts address broad public policy issues relating to the privacy of individual information and its protection which we believe will be of interest to our readers.

Three technical research articles follow. In "Releasing Microdata: Disclosure Risk Estimation, Data Masking and Assessing Utility," Natalie Shlomo provides a systematic and up-to-date look at the applicability of disclosure limitation techniques emanating from the statistical community in the context of the release of sample data files from government statistical agencies. In "On the Difficulties of Disclosure Prevention in Statistical Databases or The Case for Differential Privacy," Cynthia Dwork and Moni Naor begin with a definition from Tore Dalenius' classic 1977 paper on statistical disclosure limitation[1] and demonstrate why his goal is impossible to achieve. They describe the notion of differential privacy and a strong *ad omnia* privacy which, intuitively, captures the increased risk to one's privacy incurred by participating in a database. In "Releasing Private Contingency Tables," Shubha Nabar and Nina Mishra evaluate the method of cell suppression widely used by statistical agencies for disclosure protection in the release of two-way contingency tables, showing that the decision to suppress a cell can itself disclose information. They then provide a cell suppression algorithm for the special case of Boolean private attributes where suppressions provably do not leak information.

*Department of Statistics, Machine Learning Department, Cylab, and i-Lab, Carnegie Mellon University, Pittsburgh, PA, mailto:Fienberg@stat.cmu.edu

[1]Dalenius, T. (1977). "Towards a Methodology for Statistical Disclosure Control." *Statistik Tidskrift*, (5):35–64.

© 2010 by the authors