

Introduction to the Minitrack on Information Technology and Social Accountability

George T. Duncan and Stephen F. Roehrig
Carnegie Mellon University
The Heinz School of Public Policy and Management
Pittsburgh, PA 15213
gd17@andrew.cmu.edu
roehrig@andrew.cmu.edu

The "Information Age" has given us new technologies promising the benefits of data on demand, access to information and tools which were previously unavailable or difficult to use, and a sense that the world is at our fingertips. But benefits do not come without costs, including costs beyond the obvious financial ones. Many people are understandably concerned that new information technologies might have a negative impact on their work and personal lives. Much of this concern involves a tension between access to information and privacy concerns. The goal of this Social Accountability minitrack is to provide a forum for scientists knowledgeable in IT to contribute to an understanding of potential societal effects of IT, and to devise and propose solutions for achieving satisfactory resolution of this fundamental tension.

In this first year of the mini, we make a beginning by presenting four papers investigating techniques for ensuring privacy and confidentiality in network and database settings. The paper by Cranor and Cytron considers ways of conducting anonymous surveys, elections and the like over networks, using blind signatures for security. The paper is valuable in that it provides a concrete set of desiderata for such systems, and describes how an actual implementation (called "Sensus") measures up to them.

The paper by Fan and Lei ("Secure Rewarding Schemes") also deals with privacy in networked settings. The goal here is to provide a secure means to reward information providers, without compromising the provider's identity. As in the Cranor and Cytron paper, blind signatures are used as part of the security system.

Confidentiality may be compromised in other ways, most notably through the collection and dissemination of personal data by government agencies and others. The papers by Mukherjee and Duncan, and Duncan *et al.*, address this issue. Data collected for the public good must be published to realize its value, yet the respondents must remain anonymous. One method for protecting respondents is to add zero-mean random noise to the data; this leaves it useful for statistical purposes, but adds uncertainty which protects the individual. In their paper, Mukherjee and Duncan add a more powerful weapon to the data-masking arsenal. Since data outliers are in many ways more susceptible to inadvertent disclosure, the protection scheme proposed by them pays special attention to such outliers, giving them additional protection in the form of a larger predictor variance.

The paper by Duncan *et al.* ("Cell Suppression to Limit Content-Based Disclosure") considers the situation in which multiple data tables, each innocuous by itself, can be combined to reveal confidential information. Cell suppression, another common protection mechanism for published data, is employed to eliminate disclosure while maximizing the utility of the released tables.

Taken together, these papers provide a glimpse of a research area which is important today and which will, we think, be even more important in the future. Information technology continues to advance at an exponential rate, providing new capabilities both good and bad. As technologists our responsibility is to ensure that the advantages of IT remain available, but that any disadvantages be overcome.