3-1-2005

Transparency in InfoSec Design

Herbert Mattord
hmattord@kennesaw.edu

Michael Whitman

TRANSPARENCY IN INFOSEC SYSTEM DESIGN

Herbert J. Mattord
Kennesaw State University
hmattord@kennesaw.edu

Michael E. Whitman
Kennesaw State University
mwhitman@kennesaw.edu

Abstract

Sed Quis Custodiet Ipsos Custodes?
(But who will guard the guards themselves?)
—From Satires (c. 120 ad) by the Roman author Juvenal
(DECIMUS JUNIUS JUVENALIS, C. 60–140 AD)

Information system capabilities continue to expand. In two particular areas, that of the surveillance records and personal data, a public policy debate is underway. This debate regards the relationship between the rights of the individual to freedom from unwanted observation and the rights of the organization to collect and use data for its own legitimate purposes. This discussion encompasses privacy as well as a broader concern with what life could be like in a surveillance-based society. The fundamental question facing information systems designers is whether or not to use the contemporary approach of striving for secrecy, or to look for some novel way to assure security and privacy without secrecy. Future systems will implement surveillance and data gathering capabilities far beyond those in use today, and thus these systems will pose new challenges to our current thinking about privacy. The phrase from Juvenal, But who will guard the guards themselves? encapsulates the problem presented when any person or small group has been assigned to roles that give decision-making powers or control over wealth. Those who are trusted to protect the common good are faced with the temptation of abusing their positions for personal gain. The challenge that faces the designers of such information systems is to make sure that the resulting systems perform as designed while also meeting security and transparency needs. Balance is needed, even when systems are designed with full transparency in mind. Limits on transparency are needed to assure fairness to all concerned. The interest of the individual's need for privacy is balanced against the interest of the collective's need for transparency. While the collective needs to acquire and use information to coordinate and control the overall activities, the individual seeks to control how and to what purpose the information collected about him or her is used.