Inside Risks | Barbara Simons and Eugene H. Spafford

Risks of Total Surveillance

The U.S. Public Policy committee of ACM (USACM) is concerned the proposed Total Information Awareness (TIA) Program, sponsored by the Defense Advanced Research Projects Agency, will fail to achieve its stated goal of "countering terrorism through prevention." Further, we believe the vast amount of information and misinformation collected by any system resulting from this program is likely to be misused to the detriment of many innocent American citizens. Because of serious security, privacy, and personal risks associated with the development of any vast database surveillance system, we recommend a rigorous, independent review of TIA. Such a review should include an examination of the technical feasibility and practical reality of the entire program.

Security Risks. The state of the art in computer system design is such that any systems resulting from TIA are unlikely to be able to preserve integrity and keep data out of unauthorized hands, whether they are operated by governmental or commercial organizations. Frequent reports of successful hacker break-ins, insider misuse of supposedly secure systems, and the pervasive existence of software flaws indicate we are unable to make these systems adequately secure, and suggest the likelihood of a trustworthy database system emerging from this effort is vanishingly small.

The databases proposed by TIA would also increase the risk of identity theft by providing a wealth of personal information to anyone accessing the databases, including terrorists masquerading as others. Recent incidents involving about 500,000 military-relevant medical files and 30,000 credit histories are harbingers of what may be in store.

Privacy Risks. The need for oversight and control is especially great when aggregation and analysis of personal information is done without the knowledge or consent of the people being monitored. It is misleading to suggest that "privacy enhancing technologies" within TIA can somehow protect people's privacy, because by definition surveillance compromises privacy. Furthermore, the secrecy inherent in TIA implies citizens could not verify the information about them is accurate and shielded from misuse. Worse yet would be the resulting lack of protection against harassment or blackmail by individuals who have inappropriately obtained access to an individual's information, or by government agencies that misuse their authority.

Personal Risks. TIA would combine automated data mining with statistical analysis, thereby resulting in some number of false positives—risking incorrectly naming someone as a potential terrorist. As the entire population would be subjected to TIA surveillance, even a very small percentage of false positives would result in a large number of law-abiding Americans being mistakenly labeled. TIA would impact the behavior of real terrorists and law-abiding individuals. Real terrorists are likely to go to great lengths to make certain their behavior is statistically normal; ordinary people are likely to avoid perfectly lawful behavior out of fear of being labeled un-American.

We appreciate that the stated goal of TIA is to fund research on new technologies and algorithms that could be used in a surveillance system in the service of eliminating terrorist acts. However, we are extremely concerned the program has been initiated (and some projects already funded) apparently without independent oversight and without sufficient thought being given to real constraints—technical, legal, economic, and ethical—on project scope, development, field testing, deployment, and use. Consequently, the deployment of TIA, as currently conceived, would create new risks while providing only the appearance of increasing homeland security.

There are important steps the government can take now to increase our security without creating a massive surveillance program that has the likelihood of doing more harm than good. Federal, state, and local governments have information systems in place that could play major roles with highly focused terrorist spotting. However, many of these systems are only partly functional and/or being ineffectively used. An example is the computer system run by the Federal Bureau of Alcohol, Tobacco and Firearms which, according to the *New York Times*, was unable to link bullets fired in three sniper shootings in Maryland and Georgia in September 2002. Serious improvements in the use of current operational systems could significantly enhance homeland security without creating the major risks noted here.

BARBARA SIMONS AND EUGENE H. SPAFFORD are co-chairs of USACM. This column is derived from a USACM letter to Congress: www.acm.org/usacm/Letters/tia_final.html.

PAUL WATSON