A Global Audience Deserves a Global Perspective

THE "VIEWPOINT" BY NORMAN Matloff ("Globalization and the American IT Worker," Nov. 2004) was offensive and its publication in *Communications* inappropriate. Its point was impossible to miss: The U.S. should take action to preserve its economic superiority in IT, as well as its superiority in innovation. High-paying, high-technology jobs should be kept in the U.S. and go to U.S. nationals.

Matloff is entitled to his concerns and opinions, but publishing in *Communications* is not a neutral act. Almost as offensive is the fact that the phrase "the national economy" was used to describe the column in the executive editor's "Editorial Pointers" introduction to the entire issue.

ACM is an international organization with an international membership. Its mission statement says "... [the ACM is] dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests" and "... by promoting the highest professional and ethical standards." *Communications* and its staff have a responsibility to all members of the ACM. I urge them to be cognizant of this responsibility and be especially sensitive to the issue of U.S.-centrism.

SERDAR TASIRAN
Istanbul, Turkey

Author Responds:

TASIRAN'S REFERENCES TO "U.S. economic superiority" misinterpret the points I made in my "Viewpoint." I am highly supportive of the efforts of other countries to establish strong IT capabilities, for both internal and export purposes. For instance, I have close personal connections to China and have long been supportive of IT development there. My concern is that if current trends continue, the U.S. will not have much IT capability left itself.

Tasiran believes that *Communications,* as part of an international organization, should not have invited me to write my "U.S.-centric" piece. He has a valid point there. But I would point out that *Communications* had earlier published another "Viewpoint" on offshoring ("What Global Sourcing Means for U.S. IT Workers and for the U.S. Economy," July 2004) by Catherine L. Mann, taking a pro-offshoring perspective. That piece was equally U.S.-centric in title, language, and theme yet did not seem to draw objections as being "U.S.-centric."

NORMAN MATLOFF
Davis, CA

Blogs No Threat to Democracy

RATHER THAN LOOKING AT real-life blogs before drawing his conclusions about the alleged dangers to democracy from the Internet, Cass R. Sunstein ("Democracy and Filtering," Dec. 2004) offered a thought experiment having nothing to do with the actual blogosphere. Far from isolating visitors and readers by presenting only one viewpoint, the most popular blogs contain link after link to other sites offering diverse opinions. Many blogs support comment pages where readers post both praise and criticism. Blogs as a whole are overwhelmingly more honest than, say, CBS News in presenting not only arguments for their viewpoints but against them as well—and in

PAUL WATSON

promptly correcting themselves when others point out factual errors.

I consider it bizarre to view the empowering technology of the Internet and the blogosphere as a threat to democracy.

DANA HONEYCUTT
San Diego, CA

Author Responds:

HONEYCUTT IS RIGHT TO imply that whether blogs contribute to or instead counteract group polarization is indeed an empirical question. Unfortunately, he presents no evidence on how to answer, relying instead on his own personal observations. I am unaware of any systematic data as to whether blogs and their readers expose one another to diverse views or tend to be used to reinforce what people already believe.

Even a casual look suggests that the picture is complicated. Some blogs do expose people to new and challenging ideas, offering links to diverse views, but there are lots of echo chambers out there. On balance, the Internet and the blogs seem to me very good for democracy, but the risk of polarization is real, and we need to know more about them.

CASS R. SUNSTEIN
Chicago

Internet Voting *Not* Impossible

THE ARTICLE "ANALYZING Internet Voting Security" by David Jefferson et al. (Oct. 2004), which explored the Secure Electronic Registration and Voting Experiment (SERVE) Internet voting system, was highly critical of Internet voting, generally advising readers not to use the technology due to its inherent vulnerabilities. However, in The Netherlands, we've had a positive experience with online voting and wish to provide a more balanced view of the field.

Jefferson's article made two main arguments against Internet voting:

It risks the buying and selling of votes. But this risk holds for any voting system in which voters might vote at home. Internet voting would be more fairly compared to postal ballots, rather than voting at polling stations. If we want home voting, measures can be taken to make it unattractive to buy or sell votes.

It's vulnerable to attack. Although we recognize that the Internet is a hostile environment, a system called RIES, developed for elections involving public water management authorities in The Netherlands gives us confidence that voting systems can be protected from attack. RIES has two main protection features:

A reference table. A reference table is published before an election, including (anonymously) for each voter the hashes of all possible votes, linking them to the candidates. The number of voters in the table can be compared to the number of registered voters.

Two verifications. A document with all received votes is published after the election, allowing two important verifications: Voters can verify their own votes, including their correspondence to the chosen candidates, and anyone can perform an independent calculation of the result of the elections based on this document and the reference table published before the elections.

If a vote has been registered incorrectly or not at all, a voter would be able to detect it. If the result is incorrect, given the received votes, a voter would be able to detect it as well.

The system's main technical feature is its clever use of hash functions. Whereas the hashes of all possible votes are public, deducing valid votes from them is impossible without the required voter key. The relationship between the voter and the voter key must not be stored anywhere, just as in bank access codes; therefore, we can infer that the related procedures already exist.

The RIES system was developed by the public water management authority of Rijnland and Mullpon and is expected to be patented. It has performed well in at least one election involving 70,000 voters. Although Internet voting should not be the only way to vote in an election (due to accessibility issues and possible denial-of-service attacks), it is still feasible, as long as it does not have to be more secure than other current systems.

WOLTER PIETERS
Nijmegen, The Netherlands
JOSEPH R. KINIRY
Dublin, Ireland

Don't Trade Privacy for Security

Peter G. Neumann postulated in his "Inside Risks" column "The Big Picture" (Sept. 2004) that privacy must be sacrificed for greater security. However, current research shows that information can be shared in ways that both maximize business value and guarantee the security of the underlying mechanisms and technology while preserving privacy.

Rigorous studies of computing resources designed to secure operations have yielded empirical evidence that sacrificing privacy does not necessarily ensure greater security. For example, Sovereign Information Integration (SII) technology, developed by the Intelligent Information Systems group at IBM's Almaden Research Center, demonstrates that useful, security-focused operations can be performed in a way that preserves privacy.

SII allows two or more entities to share data without compromising the privacy or security of either data set. It computes query results across autonomous data sources without revealing anything except the results of the computation. The core principle is that two or more commutative encryption functions can be applied independently to unique identifiable data in different orders at different locations, and that the resulting doubly encrypted values can be compared without violating disclosure rules.

SII technology is broadly applicable in many fields, including medical research. For instance, a medical researcher may suspect that patients with a certain DNA sequence will react adversely to penicillin. To verify this hypothesis, the researcher needs information from hospital databases and gene bank databases—two legally separate entities with security and privacy restrictions on data disclosure and use.

Assuming the research facility runs an SII client application, the hospital would keep a copy of its patient database locally, and the gene bank would keep its database of DNA sequences and reactions at its own central data warehouse. The hospital and gene bank can simply add SII middleware to enable the SII client to perform this collaborative operation in a way that preserves privacy.

The client application then sends the request to the hospital's SII middleware. The hospital encrypts the patient table with its own key and sends it to the middleware, which encrypts the hospital's patient table and its own DNA table with its key. Both tables are sent to the hospital middleware, which encrypts the GeneBank-encrypted DNA table, does the join on both doubly encrypted tables, and sends the result back to the client application.

SII is an effective platform for security-oriented projects for a number of reasons:

- It does not require a trusted third party;
- It is a lightweight, scalable, middle-tier solution;
- It integrates transparently and seamlessly into existing security solutions;
- Its Web services query interface allows for easy integration into any application on any platform; and
- It ensures that the privacy of individuals excluded from the results of collaborative operations are not violated.

Today's technological environment offers solutions, including SII, that allow organizations to conduct business without infringing individual privacy or civil liberties. Thus, the generally held view that sacrificing privacy leads to greater security should not be promoted.

Tyrone Grandison
San Jose, CA

Author Responds:

Grandison presents a reasoned example of how privacy need not be sacrificed for computer security (I never suggested it did) but seems to have missed the bigger picture. Privacy is often compromised by trusted insiders, as well as by outsiders, able to penetrate system security. Moreover, homeland security is a very different kind of security not addressed by Grandison's reasoning. We must be careful not to mix apples and oranges.

Peter G. Neumann
Menlo Park, CA

Please address all Forum correspondence to the Editor, *Communications*, 1515 Broadway, New York, NY 10036; email: crawfordd@acm.org.