A Scientist's View of Government Control Over Scientific Publication

Peter J. Denning

This essay is based on my remarks at a session entitled "Striking a Balance: Scientific Freedom and National Security," on January 7, 1982, at the annual meeting of the American Association for the Advancement of Science (AAAS).

Other members of the panel were: Mary Cheh, associate professor of law at George Washington University; Harold Green, attorney and professor emeritus of law at George Washington University; Bobby Inman, Deputy Director of the CIA; Daniel Schwartz, attorney and former counsel to the National Security Agency; Congressman Paul McCloskey (R.-California), and Gerald Sturgis, staff member of the House Government Operations Committee.

Although my remarks are directed toward an issue before the U.S. Government, the principles herein apply in every country.

A new protectionist mood is growing in Government. To reduce the risk that an open scientific discovery might harm the national security or help a foreign country close a commercial gap, efforts are being made to apply U.S. export control laws to all forms of scientific publication, whether verbal or written. Some examples:

- Early in 1980 the Commerce Department instructed the organizers of a symposium on bubble memories, sponsored by the American Vacuum Society, to disinvite delegations from Eastern bloc countries and China. After the State Department intervened, Commerce allowed the Chinese to come but required them to sign nondisclosure agreements.

- Attempts have been made to prevent non-U.S. students from attending certain technical seminars at the universities in which they are enrolled.

- In 1978 the Government slapped secrecy orders on two applications for patents on cryptographic devices by computer scientists, but later withdrew the orders. An employee of the National Security Agency (NSA) attempted to prevent disclosure of new results at an IEEE symposium in 1977; although he was acting on his own, his action caused much alarm in the research community. The NSA attempted to get NSF to share responsibility for funding cryptographic research with NSA; this too led to misunderstanding and consternation. At the NSA's request the Public Cryptography Study Group was formed in 1980; this group has since made a recommendation for a voluntary system of prepublication review of papers on cryptography. [See *Communications of the ACM*, July 1981, pages 434–450].

- The Government is seriously considering including major portions of software technology such as life cycle management development tools and large software maintenance on the Military Critical Technologies List (MCTL). (Until the revised MCTL is published, however, we won't know the outcome.)

- A bill (*H.R. 109*) was introduced in the 97th session of Congress (1981) that would extend the "born classified" concept of the Atomic Energy Act to all categories on the Military Critical Technologies List. It would give the Government the power to prevent publication of materials deemed threatening to the national interest. [See *Communications*, July 1981, page 409.]

The export control laws are an attractive vehicle for extending the Government's protective influence because it is easy to argue that publication in international journals is a form of export. This line of reasoning is worrisome.

Because our military strength and commercial edge depend so strongly on computing, it is impossible for the computing community to avoid this issue.

In a recent ACM Forum, Fred Weingarten discussed cryptographic research in the computer science

community [*Communications*, December 1981, p. 851]. He wondered whether export controls are even central issues. He wrote: "It seems somewhat bizarre that we should be discussing limiting the export of technological information, when the Government really does not seem convinced that producing it is very important at all. We worry on one hand about all those foreign students carrying information out of the classroom, but cut funds to support American students' attendance in the same class, and limit the production of new, supposedly valuable information." I agree that the confusion about export controls is a piece of a larger problem, the lack of a clear Government policy toward scientific research. Nonetheless, a discussion of a piece may shed light on the whole.

Secrecy vs. Openness

Strong principles seemingly clash on this issue: the goal of a strong national security, the goal of scientific freedom, and the goal of the free and open market. In fact, these principles are compatible. The true clash is between secrecy and openness. With few exceptions, scientific research is most likely to strengthen the national security if it is open.

There is needed a clear evaluation of the costs of achieving these goals with and without Government control of scientific publication. (Except for atomic energy, the Government has no real control over scientific publication.) In an article for *Technology Review*, October 1981, Edward Teller argues that the limitations we impose on ourselves by restricting information are far greater than the advantages gained by others in copying our ideas. I argue further that the cost to our economic power that would be wrought by successful control on the free flow of scientific information is far greater than any reduction in risk to national security that might result from such controls.

How much control would Government have to exert over scientific publication to achieve a *significant reduction* in risk to the national security? It would be considerable. Far-reaching measures would be required to completely screen all items submitted to conferences or journals and to clear the many referees involved. Informal distribution of unpublished technical reports would have to be monitored. Scientists (and engineers) would have to obtain export licenses to travel abroad to give talks or present papers; in sensitive areas they would be required to rehearse their talks before Government agents as part of the approval process. Noncitizens would be carefully screened before being allowed to scientific meetings, research labs, or universities. These measures would have to be applied uniformly toward *all* countries—including allies—to effectively reduce information flow to the few who threaten U.S. security.

The required system is clearly more compatible with a dictatorship than a democracy. It probably would not obtain the cooperation of scientists. It would discourage young people from entering scientific careers.

Such extremes would produce side effects whose cost exceeds the benefits of the measures themselves. Scientific secrets do not keep. By depriving ourselves of efficient access to scientific knowledge, we would undermine the central reason for our technical leadership over those who threaten our security. Moreover, major efforts at scientific secrecy would harm relations with our allies, among whom cooperation is important in a troubled world. As in atomic energy, security regulations would drive wedges between civilian and military research, limiting the effectiveness of both.

The "born classified" principle began with the Atomic Energy Act of 1946. The policy of nonpublication of atomic energy papers prior to this worked because the small nuclear science research community that existed around 1940 voluntarily agreed to secrecy as part of the war effort. The Government has controlled all research in nuclear energy ever since. Other countries have done likewise.

The rest of science cannot be retrofitted for the born-classified principle. As noted above, our citizens are not likely to cooperate. Even if they did, other countries are not likely to follow our lead and subject their computing research to such controls. (Would we eventually plan *import* controls to keep foreign ideas out?)

Free exchange of scientific ideas is an essential part of technology transfer. New ideas reach industry directly, through our many journals, and indirectly, through the students who take them from classroom to employer. The economic leadership of the United States is in no small measure attributable to the most effective system of technology transfer in the world. A policy of secrecy would seriously weaken this system.

To maintain our security and economic leadership, we must promote free exchange of ideas, promote effective technology transfer, and promote public support for science. This can be done only through a policy of openness—the current policy.

In short, stanching scientific ideaflow is far more likely to hurt the national security than to aid it. Openness expedites technology transfer and strengthens our economy; secrecy confines expertise and stifles innovation. Openness encourages cooperation; secrecy breeds conflict and distrust. Openness lowers public fears of science; secrecy raises fears.

In Search of a Solution

I have heard suggestions that the potential conflict between the Government and the scientific community could be avoided by keeping defense-related research out of universities. I don't see how this could work. The Defense Department has keen interest in computer research, it has money, and it can find much of the needed expertise in universities. Moreover, as has been well illustrated with cryptography, many problem areas arising in civilian computing also arise in military computing. It therefore seems unrealistic to hope for complete separation between civilian and military research.

Should we educate non-U.S. scientists by admitting them as graduate research assistants in our universities? Assuredly yes! Those who regard foreign students as threats to security should reflect that these students contribute to *our* body of knowledge while on our soil. Half-joking, Bob Hope once used to remark that our space program was better than our competitor's because

our German scientists were better than their German scientists. The surest path to success is to get the smartest people working *for* you.

In answering a question at our session, Admiral Inman expressed his belief that future Congressional hearings on "technology transfer" will reveal examples in which adversaries obtained important ideas from U.S. scientists publishing in international journals. He suggested that such examples may provoke legislative overreaction. Even so, I believe that the scientific community should welcome hearings, which would give a full public airing of all sides of this thorny political problem.

Admiral Inman believes that cooperation between Government and the scientific community is preferable to regulatory control. He cited the voluntary system recommended by the Public Cryptography Study Group as a possible model for ensuring that national security is considered during peer review. I believe this approach is worth discussing because it is compatible with the principle of openness.

While scientists are willing to restrict their publications when national security is clearly at risk, they may be unwilling to do so merely to protect a competitive commercial edge.

It is no accident that the computing field has been free of Government regulation *and* has an impressive record of accomplishment. The U.S. scientific community has a proven record of success in promoting national interests. Government intervention to reduce risks to the national security would upset this system, reduce its effectiveness, and create friction with the scientific community. This is why I believe that control over scientific publication would not significantly reduce risk to the national security but would exact a significant cost on technology and science. Edward Teller says "secrecy is the road to nowhere."

If you want to win the Indianapolis 500 Mile Race, you build the fastest car. You don't throw nails on the track.

Virtual JAM, Then and Now

Five years ago, in the July 1977 issue of this publication, I presented an editorial which analyzed the content of the previous year's volume of *Communications*. At the time the acronym associated with the "how to make CACM more satisfactory" movement was JAM, standing for Journal for All Members. The editorial specified how one might extract pages from the 1976 volume so as to obtain a publication which seemed more what the critics had been requesting. It turned out that some 500 pages, or about 60 percent of the total, could be so extracted, and since it was hoped that the extraction would be logical, not physical, the specified contained publication was termed "virtual Journal for All Members," or vJAM.

At the time this exercise was undertaken the major criticism of *Communications* seemed to be from what has been, perhaps simplistically, called the "practitioner community," that the publication was overburdened with abstruse research papers, of interest to a narrow segment of the readership. The editorial classified 48 papers appearing as Technical Contributions (in the section now called Research Contributions) as perhaps of this character, but classified 15 Technical Contributions as being, both in subject matter and readability, of interest to a more general audience. These 15 papers, together with 11 Reports and Articles and 3 Student Award papers, constituted about 40 percent of the vJAM page count, the rest being the Departmental Features (Forum, Professional Activities, etc.) and advertising (which itself was a little over 20 percent of the total). Because it was recognized that this classification was subjective, depending on the judgment of the Editor-in-Chief, the 15 Technical Contributions were listed by title, along with the Reports and Articles, so that the critics could venture their own opinion as to whether vJAM did or did not live up to its billing. No such opinions were ever ventured, however, either in letters submitted to the Forum or otherwise.

In the intervening five years the ACM Publications Planning Committee has laid out a course to be followed, and ACM publications have evolved, notably by the spinning off of *Transactions* for the specialized interests and the introduction of the Computing Practices section in *Communications*. Recently the criticism has swelled again. This time, the dissatisfaction seems to be in the "research community," who are grateful for the *Transactions* but feel that the removal of so much research material from *Communications* has left it without character (see Forum letters and editorial response, November 1981 issue, pp. 785–87). At the same time, there are at least some who seem to feel the character has not changed, a diametrically opposed position. These diverse points of view are reflected, with customary brevity, in the letters printed in the Forum for this month.

The Publications Planning Committee, in its "framework" report [1] and its first "three-year plan" [2], envisioned an evolution of *Communications* not unlike what has in fact taken place. Nevertheless, due to current feelings on the matter, the Publications Board has undertaken to present a specific plan to Council for the "revitalization" of this, the ACM flagship publication. In view of the welter of conflicting opinions and ideas circulating, it seems worthwhile to do another vJAM analysis, to at least make some data available to those who wish to become involved in the debate. Accordingly, there follows a vJAM specification for the 1981 volume of *Communications*, and a comparison with the earlier analysis of 1976.