

gated the whole thing," says Gartland. Martin did conduct an investigation, and he took action both with the NIH and the insulin team. "I felt comfortable we had resolved the question and eliminated the possibility of it happening again," he says. But in fact, written documents of the committee record criticism only of the NIH.

The pBR322 experiment raises no question of hazard but it does raise the possibility that the insulin team might have gained an unfair advantage over other researchers who had abided by the NIH rules. Another team at Harvard is also working on the same problem.

Members of the UCSF team say that they gained no information from the pBR322 experiment which was helpful to the later experiment with pMB9. As it happens, the Harvard team was not neck-and-neck with UCSF because it has not even now published any results.

As far as is known the pBR322 experiment is the only occasion on which the NIH rules governing recombinant DNA research have been broken. The researchers say that the breach was the result of innocent error, a statement not refuted by the available evidence. The experiment presented no hazard to public health nor, in the event, was

any unfair advantage gained over competitors. As for the UCSF biosafety committee, its response included action to ensure against repetition of the incident, although not a full public account. The committee's discussion of the experiment, as reflected in the minutes of its 20 May meeting, is confined to an attempt—unsupported by available evidence—to ascribe the error to confusion generated by NIH. But both the experiment and the biosafety committee's response to it occurred in circumstances to which researchers were then still adapting, and for which there were few, if any, precedents.—NICHOLAS WADE

## Cryptology: Scientists Puzzle Over Threat to Open Research, Publication

A group of university and industry scientists who are planning a symposium on cryptology have found themselves victims of a bizarre threat from an employee of the National Security Agency (NSA), the government's code-building and code-breaking agency, which says that they may be violating federal laws. And, while the scientists have declared they are not intimidated and will proceed with the symposium, the incident has brought out an unanticipated conflict between researchers' rights to academic freedom and the NSA's job of protecting national security.

Historically, primarily the intelligence community has been interested in cryptology, and it has tended to keep the subject under a tight blanket of secrecy. But in recent years, a number of developments have combined to bring the subject out, so to speak, into the open. One development is a growing corporate interest in secure telephone and data communications. A second is the discovery by scientists doing basic research in mathematics, engineering, and computer science that recent results in these fields can be applied to devising what may be virtually unbreakable codes. The result is that a new field of civilian research has sprung up on this traditional military preserve.

The new research involves both ways to break existing codes and ways to make new codes that are, for all practical

purposes, unbreakable. The new codes have generated intense interest among the scientists because they are based on a collection of mathematical problems which can only be solved by running computers continuously for years or even for decades. The only known way such codes can be broken is by solving one of these problems. Interest in these "unsolvable" problems has also sparked discussion among the scientists about the vulnerability of existing coding schemes developed by the government—specifically the NSA and the National Bureau of Standards—and approved for commercial use and foreign export (*Science*, 29 July 1977, p. 428).

The cryptology symposium that has come under fire has been arranged under the auspices of the Information Theory group of the Institute of Electrical and Electronics Engineers (IEEE)—the nation's largest engineering professional society—and is scheduled for 10 October in Ithaca, New York. Prominent among those who will be speaking and presenting papers are Martin Hellman of Stanford University, Ronald Rivest of the Massachusetts Institute of Technology (MIT), Aaron Wyner of Bell Laboratories, and other researchers at IBM, Cornell University, and Ohio State University. As an IEEE symposium it will be open to the public, and a number of foreign guests and participants are expected to attend. In addition, there had

been plans to send preprints of the talks to the Soviet Union, under a general umbrella agreement the IEEE made a few years ago with the Soviets. (But this agreement has never been implemented.)

The Information Theory group was preparing for the session as any group of scientists would when, in August, they were sent a mysterious, single-spaced, one-and-one-half-page letter which argued that both to publish in the field of cryptology and to export such publications could violate the 1954 Munitions Control Act (now revised as the Arms Export Control Act). This is the law by which the federal government, through the Department of State, regulates the flow of weapons, computers, and other sensitive equipment to foreign countries.

The letter, from J. A. Meyer at a Bethesda, Maryland, address, argued that several of the group's past, present, and future activities could violate the rules—the International Traffic in Arms Regulations (ITAR)—by which the State Department implements the provisions of the act. It cited the forthcoming Ithaca symposium, a past symposium held at Ronneby, Sweden, several publications in which articles by Hellman had appeared, and the plan to send preprints to the Soviet Union.

Meyer warned the IEEE scientists with sentences such as: "I assume the IEEE groups are unfamiliar with the ITAR, which apply to the publication and export of unclassified as well as classified technical data. . ." and "[A]tomic weapons and cryptology are also covered by special secrecy laws."

The letter also ended with an ominous paragraph:

"Superficially, it appears that a small number of authors are providing most of the papers and most of the motivation. They may not be aware of the full burden of government

controls. Some of the topics addressed, e.g. the DES algorithm, are intended for U.S. government activities and . . . unless clearances or export licenses are obtained . . . or there is some special exemption, the IEEE could find itself in possible technical violation of the ITAR. . . . As an IEEE member, I suggest that the IEEE might wish to review this situation, for these modern weapons technologies, uncontrollably disseminated, could have more than academic effect.

Meyer enclosed sections of the ITAR rules, and the IEEE, after replying that it had determined its publications were exempt, forwarded the letter and enclosures to the Information Theory group

scientists. However, in doing so, the IEEE Director of Technical Activities, Nirendra P. Dwivedi, appeared to accept the Meyer letter and its chilling interpretation at face value and put IEEE's implicit approval on Meyer's interpretation of the law. Dwivedi's letter to the scientists urged them to clear any papers they planned to present with their companies. If they had no other way to clear their work, "the authors should refer the paper to the Office of Munitions Control, Department of State, Washington, D.C., for their ruling."

The scientists were predictably star-

tled by the sudden revelation that they could not publish in their field of study without first consulting the State Department. Says the Information Theory group's president Fred Jellinek, "I don't believe a law can say such a thing, because it would make scientists guilty until proven innocent."

Other scientists, such as Hellman of Stanford and Rivest of MIT, turned the problem over to their universities' lawyers and opted to lie low until the lawyers finished looking into the issue. Hellman says he is 99 percent sure he will participate in the October meeting—un-

## Briefing

### FTC Sues AMA over Code of Ethics

After nearly 2 years of pretrial legal skirmishing, a big battle has begun between the Federal Trade Commission (FTC) and the American Medical Association (AMA). Leading the charge for the FTC are five young attorneys from the Bureau of Competition, who claim that provisions of the AMA code of ethics have inhibited medical innovation and led to higher health costs. The objects of the attack are AMA bans on advertising and on contractual arrangements that physicians may make with third parties.

The testimony before assistant chief administrative law judge Ernest Barnes has been notably undramatic, but the impact of the suit on the 200,000-member AMA and on health care in the U.S. may be far-reaching. The charges themselves are considered to be the most serious leveled against the AMA since it was convicted of a criminal antitrust conspiracy to restrain competition in 1943.

The FTC seeks nothing less than a complete cessation of professional restrictions of advertising, even of ads that seem false or deceptive to the AMA. The agency also wants an end to AMA bans on physicians' contracts with lay organizations and nonphysician health professionals. Both remedies would dramatically alter the picture of U.S. health care.

To defend itself from such changes, the AMA has engaged the legal services of Newton Minow, a former chairman of the Federal Communications Commission (FCC) and no stranger to regulatory law. The defense Minow has prepared will emphasize the voluntary nature of AMA membership and will contend that its

advertising ban protects the public from charlatans.

On the other side, witnesses for the FTC will relate tales of harassment by AMA's constituent (state and county) societies of those who refuse to tow the AMA line. Two doctors from Connecticut and Massachusetts, for example, will testify about sanctions applied against them after local newspapers published articles about their use of Kelman Phaco-Emulsifier-Aspirators, new machines used in cataract surgery. Another doctor from West Virginia will testify about his attempt to establish a partnership with a physician's assistant, and the AMA's advice to him that the partnership would be unethical.

The suit is only one manifestation of growing FTC interest in possible anti-competitive behavior by professional and trade associations. In the health area alone, the FTC already has issued a complaint against the American Dental Association and is looking into physician control of Blue Shield plans, restrictions placed on Health Maintenance Organizations by various groups, and AMA control over the supply of physicians and health care services through definitions of practice and school accreditation.

The agency's interest in professional groups was aroused by a decision of the U.S. Supreme Court 2 years ago in *Goldfarb v. Virginia State Bar*. In the decision, the Virginia State Bar was held in violation of antitrust laws for ethical principles preventing lawyers from regularly charging less than the bar's schedule of minimum fees.

As a lawyer for the FTC put it, "Before *Goldfarb*, we didn't think we had the jurisdiction—now that we do, we'll be taking a good look at all of these associations and their high-flown 'ethical' principles."

### Public Gains Access to Pesticide Safety Data

In an important move, the House agricultural oversight subcommittee on 15 September unanimously accepted a proposal to require pesticide safety data filed with Environmental Protection Agency (EPA) to be available for disclosure to the public. To the delight of environmentalists, the subcommittee rejected an industry-sponsored plan to restrict severely the data's availability. Environmentalists have sought access to such data to verify—or challenge—industry safety claims.

Currently, companies registering pesticides with the EPA under provisions of the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) have the right to refuse requests for the registration data under a provision protecting "trade secrets." On several occasions, pesticide companies have claimed that environmental impact data fall under the aegis of trade secrets; in a recent case involving the pesticide chlorobenzilate, the EPA and the Environmental Defense Fund went to court to claim that the safety data are not trade secrets.

The subcommittee gave chemical companies proprietary rights to manufacturing data, but they rejected a proposal by Representative Charles Thone of Nebraska to allow only "qualified scientists, upon request and for good cause" to review and not copy the safety data. Under the new amendments to FIFRA passed by the subcommittee, the secrecy limitation on registration data will apply only to requests from private companies with financial interests in the information, and safety data, excluding any information on deliberately added inert ingredients, will be available to the public.

less, that is, the Stanford lawyers find some legal problem or if Stanford will not defend him should one later arise.

Rivest found himself in an embarrassing situation, since the August 1977 *Scientific American* had published a very detailed description of his scheme for an unbreakable code (also described in *Science*, 19 August 1977, p. 747) with an offer that he would send his paper to anyone who asked. At the time he was warned by Meyer and the IEEE, Rivest was being deluged with requests for his paper. Many of the requests were coming from abroad. "If I were more of a skeptic,

I'd think I was being set up," Rivest told *Science*. Rivest is not sending the paper out until after MIT's lawyers have determined whether ITAR has any application in Rivest's case.

Until this point, the scientists had heard only rumors about who Meyer was and what might be his motives. But *Science*, investigating the incident, determined that J. A. Meyer of Bethesda, Maryland, in fact works for the NSA. *Science* contacted Meyer's office after locating his number in an NSA directory. But neither Meyer, when he was reached, nor officials of the agency, would con-

firm that he worked there. However, after *Science* determined that an NSA employee had written the letter and had so informed the NSA public affairs office, the agency responded with an official statement. Said spokesman Norman Boardman "I can state for the agency that we had nothing to do with that letter . . . Meyer wrote that letter as a private citizen. But with respect to any letter of that nature this agency would not prompt anyone to do it." (Despite his apparent knowledge of Meyer and the letter, however, Boardman would not comment on whether he had seen the

## Briefing

In a major bonus for the chemical industry and the American Farm Bureau Federation, the subcommittee also approved a provision for conditional registration of new pesticides before safety data are complete if the pesticides are similar to existing compounds. Passage of the provision reflects an effort to bail out the EPA's pesticide enforcement program for the second time since responsibility for pesticide safety was transferred to EPA from the Department of Agriculture in 1972.

Then, EPA was directed to register 1400 active pesticidal ingredients approved for 45,000 different uses, with a deadline for completion of October 1976. After an initial extension granted by Congress in 1975 until next month, it became apparent that the EPA had failed abysmally in keeping to its schedule—that safety testing of existing pesticides will take at least another decade.

A recent National Science Foundation study, for example, found that EPA had safety data on fewer than half of the registered pesticides, and that crucial data on the carcinogenic potential of many of the chemicals were missing. Moreover, only one-quarter of the pesticides in current use initially examined by the EPA were certified as completely safe.

The subcommittee, in attempting to streamline the review process, chose to lighten EPA's work load by easing the requirements for pesticide approval and by transferring primary responsibility for enforcement of regulations on pesticide abuse from EPA to the states.

Future stops for the bill are the full House Agriculture Committee, which may vote on it this week, the House floor, and a House-Senate conference committee. Both environmentalists and industry expect it to remain as approved by the subcommittee. One factor in the

mood of Congress: recent disclosures of evidence linking the soil fumigant pesticide dibromochloropropane (DBCP) to sterility in workers at an Occidental Chemical plant in California. DBCP was originally scheduled for EPA review last winter, but the review was held up because of the backlog there.

### More Fingers in the RANN Pie?

Some 6 years ago, after goading by the Nixon White House to produce more tangible returns on the investment of research dollars, the National Science Foundation (NSF) created a Research Applications Directorate, more commonly known as RANN, for Research Applied to National Needs. RANN, which now commands a \$67-million budget, has been controversial in basic research circles. Last month the National Science Board, after lengthy study, voted to drastically restructure the RANN program so as to bring it under new guidance by NSF basic researchers. Another aim of the restructuring is to strengthen the program's ties with the groups that ultimately may be able to use the knowledge and technology which it produces.

Moreover, RANN has been given a new name, the Science and Engineering Applications Directorate. Its issue-oriented divisions (resources, environment, and productivity) were scrapped in favor of two policy-oriented divisions (problem-oriented basic research and problem-focused research applications). NSF basic research directorates will provide substantial guidance for these two divisions. RANN's exploratory research division was transferred into a new division of ap-

plied research, and the intergovernmental science-incentives division was left intact.

In October, Alfred Eggers, the director of RANN until his resignation in June, will become the director of Lockheed's Palo Alto research laboratory. Eggers served as a special assistant to NSF director Richard Atkinson while Atkinson weighed the merits of alternate RANN reorganization plans suggested by a special NSF task force. The new Science and Engineering Applications Directorate is chaired by Jack Sanderson, a physicist who had been director of the NSF office of planning and resources management.

Sanderson hopes to blunt some past criticism that the targets of RANN's research were too diffuse, and the outcomes inappropriate. He plans to encourage input from basic researchers and technology users in major decisions on policy priorities. "RANN's division of productivity is an example of the shotgun approach that we've discarded," Sanderson said. The division has funded studies ranging from labor arbitration to solid waste collection.

Despite concern by Eggers that the new plan may amount to management by committee—"a lot of fingers in the pie"—sources on the Hill and in the Carter Administration are generally optimistic about the future of applied research. Sanderson has a dozen tentative new ideas for applied research, including analysis of the effects of stress on man and society, the biological impact of chemical compounds, architecture and design for human living, production automation, and the global carbon cycle.

NSF director Atkinson also has pledged up to \$10 million in discretionary funds to help get the new research under way, augmenting the directorate's \$63 million 1978 budget.

R. Jeffrey Smith

letter or whether Meyer worked for NSA.)

Still another wrinkle in the incident results from Meyer's interpretation of the rules, which IEEE and several of the scientists had accepted at face value, but which is widely disputed. For instance, James D. Hataway, the Deputy Director

of the Office of Munitions Control at the State Department, in commenting on the Meyer letter said that nearly every interpretation it makes sounded inaccurate. "Publications and material available to the public are exempt from export control rules," says Hataway.

In fact, if the scientists followed the advice of the IEEE and Meyer and sought permission from the Office of Munitions Control before meeting or publishing, the NSA would gain control over the release of their work. Munitions Control officials at the State Department (who process 23,000 requests of all types each year) say that any requests relating to encryption or cryptographic devices are referred to the NSA for rulings. Thus, Meyer was proposing, in effect, a censorship system by the NSA over the research of the Information Theory group.

While the NSA might wish to keep the current research into unbreakable codes secret—presumably to deny them to hostile countries—such coding schemes could have benefits in civilian, commercial life. Recent news stories and congressional investigations have revealed the extent of possible eavesdropping on ordinary telephone and data communications, and the demand for secure communications is growing. If everyone—governments, corporations, even private citizens—had the capability to encode their communications absolutely, all these threats to privacy would at least abate, and might just go away. In this context, the NSA's interest in denying access to the research seems rather narrow.

Whatever the motives of NSA or Meyer, the letter could point to a genuine legal problem, which revolves around whether the scientists' work constitutes something called in the act "technical data." "Technical data," in the ITAR rules, are defined as "any unclassified information that can be used, or adapted for use, in the design, production, manufacture, repair, . . . of . . . implements of war on the U.S. Munitions List."\* The official munitions list, in addition to many weapons and high-grade computers, includes "speech scramblers, privacy devices, cryptographic devices (encoding and decoding) and specifically designed components therefor, ancillary equipment, and especially devised protective apparatus for such devices, components, and equipment."† Only the lawyers will be able to opine whether the publications and the planned discussions in Ithaca could be construed as "technical data" and hence be subject to government controls.

Another question is whether the scientists can go ahead as planned, let the chips fall where they may, and still abide by the law. A footnote in the ITAR would seem to compromise their academic freedom. It says:

\*International Traffic in Arms Regulations, 22 CFR, §125.01    †ITAR, §125.01, Category XIII (b).

## OTA Council Opts for Big Names

A final list of 24 candidates for the vacant post of the director of the Congressional Office of Technology Assessment (OTA) has been drawn up by that office's science advisory council. And, to judge by the number of luminaries of academia, government, and science policy who are on the final list, it seems that the advisory board was thinking that the \$154 million per year enterprise needs an eminent outsider to untangle its current affairs.

The 24 names were culled from a much larger list, finally numbering 219 names, which had been obtained by soliciting professional societies and which was turned over to the science council, chaired by Jerome B. Weisner, president of MIT, for further sorting a few weeks ago. Now, the list of 24 has been sent to OTA's Congressional Board of Directors, which is headed by Edward M. Kennedy (D-Mass.)

Both the office and the board of directors have had their troubles lately: one of the Republican members of the board resigned protesting that Kennedy was using the board for partisan political purposes; and the office was surprised, in May, by the resignation of its Director, Emilio Q. Daddario. In addition, Congressional dissatisfaction with the way the office has been working is surfacing in the form of hearings on whether the office's founding legislation should be rewritten or changed. So, it seems, the council would like the board to pick someone who has stood aside from these problems, and who can come in and pick up the pieces. The board of Congressmen, who will make the final selection, will not be bound by this list, but it seems likely it will try to persuade at least one of the big names on it to accept the post.

The council indicated, with an asterisk (\*), which of the 24 candidates seemed "more likely" to consider taking the job.

**Lewis S. Branscomb**, vice president and chief scientist, IBM Corporation.

**Harvey Brooks** (\*), professor of Technology and Public Policy, Harvard University.

**William D. Carey**, executive officer, American Association for the Advancement of Science.

**Richard Carpenter**, senior research associate, Environment and Policy Institute, East West Center, Honolulu, Hawaii.

**Robert Charpie**, president, The Cabot Corporation.

**Lloyd M. Cooke** (\*), director of University Relations, Union Carbide Corporation.

**Ruth Davis** (\*), deputy director, Research and Engineering, Department of Defense.

**Jacob E. Goldman**, group vice president and chief scientist, Xerox Corporation.

**George R. Herbert** (\*), president, Research Triangle Institute.

**Charles J. Hitch**, president, Resources for the Future.

**Don E. Kash** (\*), director of Science and Public Policy Programs, University of Oklahoma.

**Carl Kaysen**, professor in Humanities, Massachusetts Institute of Technology.

**Franklin A. Long** (\*), Luce Professor of Science and Society, Cornell University.

**Wolfgang K. H. Panofsky**, director, Stanford Linear Accelerator Center.

**Don K. Price** (\*), dean, John F. Kennedy School of Government, Harvard University.

**Richard W. Roberts**, staff executive, General Electric Corporation.

**David Z. Robinson** (\*), vice president, Carnegie Corporation.

**John Sawhill** (\*), president, New York University.

**Dorothy M. Simon** (\*), vice president and director of research, Avco Everett Corporation.

**Russell E. Train** (\*), senior associate, Conservation Foundation, former administrator, Environmental Protection Agency.

**Weston E. Vivian** (\*), adjunct professor, University of Michigan (former Congressman.)

**Gilbert F. White**, director, Institute of Behavioral Sciences, University of Colorado.

**Carroll L. Wilson** (\*), professor, Sloan School of Management, MIT.

**Herbert F. York**, director, Program on Science, Technology and Public Affairs, University of California at San Diego. —D.S.

The burden for determining appropriate U.S. Government approval for the publication of technical data falling within the definition . . . , including such data as may be developed under other than U.S. government contract, is on the person or company seeking publication.‡

The Meyer letter also raised, but did not discuss, a second possible legal tangle, namely whether civilian work on code schemes can run afoul of federal classification laws. The scientists are now wondering whether, if they begin developing unbreakable codes or if they accidentally replicate classified work done by NSA, they will be subject to having their own work classified, too. This is the issue of "self-classification" by civilian scientists. But government self-classification policies seem unclear. There have been instances in which the Atomic Energy Commission classified a civilian researcher's work on laser fusion to the eventual consternation of a company that claimed rights to the researcher's work and that wanted to exploit it commercially.

In a more recent case, the Energy Research and Development Administration (ERDA) classified a talk on thermonuclear fusion given by a Soviet expert, L. I. Rudakov, that Rudakov had given at U.S. government laboratories (*Science*, 8 October 1976, p. 166). In that case, ERDA officials were so zealous that they even seized a blackboard Rudakov used while giving the talk. Whether NSA can or will follow similar classification policies in the current case remains unknown.

Perhaps the most telling aspect of the incident is what it may reveal about NSA policy. If Meyer is acting as an NSA agent and not as a private citizen, the incident seems to reveal that the NSA has no coherent policy to deal with research whose public dissemination may hinder national security. Although Meyer is trying to squelch the cryptology symposium, the NSA apparently said nothing about a recent issue of the *IEEE Transactions* devoted to spread spectrum communications. This subject, according to Hellman, has obvious military applications. The technique can be used to prevent or greatly reduce the effects of attempts to jam the electronic transmission of messages. It can also be used to communicate securely from behind enemy lines.

Meyer's threats to the cryptologists seem even more misdirected since it is already too late to prevent information on the new code-making techniques from becoming widely disseminated.

‡ITAR, §125.11 (a) (1).

## Einstein Skeptical of ESP After All

In 1930, Upton Sinclair wrote a book entitled *Mind Reach* about telepathy experiments he performed with his wife. The book contained an introduction by Albert Einstein. Ever since, believers in parapsychology have cited Einstein as one of their number, thereby lending credence, in the eyes of many, to this extremely controversial field.

Now, however, evidence has come to light that Einstein did not believe in parapsychology after all. Martin Gardner of *Scientific American* has obtained a copy of a letter by Einstein, written in 1946, explaining why he wrote the introduction to Sinclair's book. The letter was to Einstein's friend Jan Ehrenwald, a psychoanalyst who, according to Gardner, was a believer in extrasensory perception.

In his letter, Einstein said that he wrote the introduction because Sinclair was a personal friend. But, he pointed out, "I wrote it in such a way that my lack of conviction is not indicated, but without having to sacrifice honesty. I confess openly to you my skeptical attitudes with respect to all such beliefs and theories . . ." Einstein said he was particularly suspicious of the experiments of J. B. Rhine, in which subjects seemed to be able to communicate mentally and their ability to communicate was independent of their distance from each other. This lack of dependence on distance, Einstein wrote, "means that there is a very strong indication that a nonrecognized source of systemic errors may have been operating."

Einstein ended his letter with an expression of consternation that his words were taken so seriously. He wrote that "the public tends to give more weight to my comments than is justified, considering my ignorance of so many things . . ." His concern, apparently, was well founded, but his reputation as a parapsychology advocate may now be so firmly established that even his recently uncovered letter will have little effect.—G.B.K.

Many sophisticated scientists need only a hint of what avenues to pursue in order to develop these schemes. In November 1976, Whitfield Diffie of Stanford and Hellman published an article in the *IEEE Transactions* that exuded such hints. Among other things, Diffie and Hellman suggested that scientists try to base codes on a specific group of problems with essentially uncomputable solutions. Now, nearly a year after their article was published, Meyer warns it may be in violation of federal law. In the interim, however, the article was widely read and quoted, and it stimulated Rivest and his associates to develop their scheme. Developing new codes on the basis of the Diffie and Hellman article still requires a lot of work, Rivest points out. But the most difficult hurdle of realizing what approaches will be successful has been passed.

Another pair of reasons that it is too late to stop the cryptography results from being known are the articles on cryptology in *Science* and *Scientific American*. Both of these articles could be in violation of the Munitions Control Act, according to Meyer's interpretation of the Act, and they too have been widely read. Although Diffie and Hellman did not release one crucial aspect of their

scheme, Rivest's scheme, at least, could easily be programmed into a computer on the basis of those articles. And sophisticated engineers could make computer equipment that would automatically code and decode messages using Rivest's scheme. Moreover, Rivest says he and his colleagues purposely wrote their paper so that the scheme could be used commercially. They sent out numerous copies of the paper before they became aware of the Munitions Control Act.

One reason the NSA seems to follow such a confused and ineffective strategy in monitoring research publications may be that it is sometimes difficult to know which germ of an idea will grow to threaten national security. The agency may have believed that Diffie and Hellman's ideas would not pan out for years, if ever. But Rivest and his colleagues exploited one of those ideas almost immediately, and their work received widespread publicity. The footnote to the Munitions Control Act, then, may be nearly useless in many cases—not because it is unenforceable but because no one, not even the generously funded NSA, can have the foresight to decide which ideas should be kept under wraps.—DEBORAH SHAPLEY and GINA BARI KOLATA