Prior Restraints on Cryptography Considered

There could be a chilling effect on mathematicians and computer scientists

Members of a public cryptography study group have decided that they want to at least consider some sort of prior restraints on the dissemination of results in cryptography research. The group is fully aware that such an unprecedented action might have a chilling effect on cryptography research and that prior restraint might even be unconstitutional. But many of the members feel that restraints may prove desirable for reasons of national security.

The study group came into being because the National Security Agency (NSA) is getting edgy about scientists' recent propensity to do research on how to make and break codes. Until just a few years ago, cryptography was the near-exclusive domain of the military and the NSA. Then, banks, corporations, and government agencies became increasingly aware that computer messages and data are insecure unless they are encrypted. In addition, electronic fund transfers and electronic mail created a vastly expanded market for cryptography. At the same time that the demand for cryptography began to grow, mathematicians and computer scientists became interested in the theoretical problems of designing and breaking codes.

The NSA, however, did not greet this public research on cryptography with any enthusiasm. Vice Admiral Bobby Inman first made the agency's consensus known about 1½ years ago (*Science*, 27 October 1978, p. 407).

Inman said that the current spate of research in cryptography caused him to have "a deep conviction that the national security missions entrusted to the agency are in peril." He explained that the NSA has two fears. First is that published results may reveal to certain countries that their codes are insecure, and lead them to change their codes to ones the NSA cannot break. The second concern is that academics may publish instructions enabling anyone to make unbreakable codes, which could greatly inhibit the NSA's intelligence-gathering function. Inman called for a dialogue between the NSA and the academic and industrial communities.

A direct consequence of this call for a dialogue was the formation of a public cryptography study group. Its members include Daniel C. Schwartz, who is the general counsel of the NSA, representatives of mathematics and engineering societies, and a representative of the American Association of University Professors (AAUP). The authorized observers include Richard A. Leibler, who is chief of the office of research at the Department of Defense.

The group had its first meeting on 29 March, at which it became clear that NSA is exploring the idea of funding all research grants in cryptography, taking this function away from the National Science Foundation. A number of the group members are concerned because many academic scientists and universities refuse to accept grants for classified work.

The group met for a second time on 29 May with the intent of discussing whether there should be limits placed on the research, development, and publication of cryptography research and whether existing regulations might not already provide some restraints.

The group was advised by Schwartz and by Ira Michael Heyman, a constitutional lawyer at the University of California, Berkeley, that existing regulations require Defense Department approval for the export of cryptologic devices but not necessarily for scholarly papers, articles, or conferences unrelated to specific hardware. Schwartz pointed out, however, that there is still some confusion over what exactly is covered in the International Traffic in Arms Regulations (ITAR), by which the State Department regulates the export of technical data and devices, such as weapons and computers. The ITAR could be interpreted as saying that research results in cryptography are "technical data" and therefore subject to export controls, which could include restricting their publication.

The problem of deciding what is "technical data" really is the problem of trying to draw a line between a theoretical result and its application. This is not so easy to do. George Davida of the University of Wisconsin in Milwaukee, who was representing the Computer Society of the Institute of Electrical and Electronic Engineers, pointed out that it is only a short step from an algorithm to a device.

As an example, Davida noted that in 1976, Martin Hellman of Stanford University and Whitfield Diffie, now at BNR in Palo Alto, published a paper on how to make a new kind of code. It took three MIT mathematicians only a couple of weeks to devise a code of the proposed sort. Now dozens of mathematicians and computer scientists are developing these codes and the MIT group is putting theirs on a computer chip. "The difference between an algorithm and a machine is trivial in practice. In order to control cryptography you would have to control basic research and theoretical developments in allied areas such as mathematics," Davida said.

Schwartz explained that the NSA's interest is in defining what Inman calls the "central core [of research] with discernible impact on national security." But the core is hard to define or defend. Schwartz and Leibler, speaking for the DOD, said that if they see an example they may be able to tell if it is part of the core, but they cannot promise to reveal why since such information is often classified.

The group decided that a subgroup should meet this summer to try to define cryptography. The group then went on to try to decide what sort of regulations restricting publications might be satisfactory. Leibler explained that "We [DOD] would like to review cryptographic articles and have some way of enforcing non-disclosure." Heyman suggested that yet another subgroup meet this summer to "put forward a schema on how prior restraints can take place." Of course, said Heyman, "What we would do with any document that came out is a big question. I could imagine a voluntary compliance scheme or an authoritative one. A lot depends on whether we could arrive at an acceptable document."

Several members, and particularly Davida, expressed grave concerns over the tenor of the meeting. What was only briefly touched on was the need for the public, and not just the military, to have secure cryptographic devices. "We are the most computerized society in the world," Davida said, and sensitive financial, personal, and corporate data are now extremely vulnerable to computer tapping. He is concerned about the chill-

0036-8075/80/0627-1442$00.50/0

ing effect that prior restraints would have on research and is concerned that this sort of effect would do far more harm to the country than a lack of restraints would do to the NSA.

George Handelman of Rensselaer Polytechnic Institute, who represented the Society for Industrial and Applied Mathematics, questioned what sort of impact prior restraints would have on universities. He said he went to the dean of academic affairs at his university and asked him what he would do if faculty members found their research was classified or, because of prior restraints, buried. Handelman said that the dean replied, "Don't let a graduate student near such research. The work is also a high risk for the untenured or for those who have promotions available."

The study group, of course, will not be the ultimate determinant of whether prior restraints are implemented. It may even prove impossible to formulate such restraints because it may be impossible to define what sorts of research are directly applicable to cryptography. And the question of whether such restraints are constitutional is still open. "I have no objection to the exercise [of considering restraints], although I find that the whole issue of prior restraint is greatly troubling," says Jonathan Knight, an authorized observer from the AAUP. But, says Knight, "I am not optimistic that we will be able to draw up anything that will satisfy these people [of the study group] with such very very diverse concerns."—GINA BARI KOLATA

Forensic Use of Hypnosis on the Increase

Researchers fear misuse by police, warn that hypnotic state is no guarantor of truth

On 10 June newspapers reported that Martha Coleman, the woman who was with civil rights leader Vernon Jordan when he was shot in Fort Wayne, Indiana, had agreed to the FBI's request that she undergo hypnosis to enhance her memory of the event.

The use of hypnosis by law enforcement agencies has become increasingly common, just as hypnosis has come back into fashion in recent years as a therapeutic modality. But there is by no means universal agreement on the credibility that should be accorded hypnosis-evoked testimony in court.

The forensic use of hypnosis has occasionally produced striking breakthroughs: in 1973, after the bombing of an Israeli bus, the driver was able to recall details about a passenger that led to apprehension of the terrorists; some years later, in Chowchilla, California, another bus driver was able to recall most of the license plate number of a van in which children had been abducted from a school bus. This year brought a particularly unusual hypnosis-aided solution to an old crime: a 44-year-old North Carolina woman was able to dredge up a repressed memory of a gruesome event 35 years before when her mother had murdered her father, chopped him up, and hidden the remains in an outhouse.

The services of professionals trained in hypnosis are now frequently sought in criminal cases where it is thought that scavenging the memory of victims and witnesses may supply new leads. It can be particularly helpful in aiding recall of emotion-laden crimes, such as rape and homicide, where psychological defenses can result in the repression of traumatic details. (Laws prohibit prosecutors from employing hypnosis with defendants.)

But although everyone agrees that the procedure can be very useful, there is considerable controversy over the extent of its usefulness and the degree to which hypnosis-evoked information can be relied on in court proceedings. Academic researchers in particular do not like the fact that law enforcement officials unschooled in psychology use hypnosis, and two professional organizations, the Society for Clinical and Experimental Hypnosis and the International Society of Hypnosis, have in the past 2 years passed resolutions avowing themselves to be "deeply troubled" by police use of hypnosis and stating that it is "unethical" to train laypersons in the procedure.

Hypnosis is difficult to define because no one really understands how it works. As Ernest Hilgard of Stanford University, one of America's foremost hypnosis researchers, says, "we don't know enough about the ordinary waking consciousness" to be able to speculate on just what sort of state of consciousness hypnosis represents. Stage hypnotists of yore imparted an unwarranted aura of glamour and mystery to the procedure, implying that the hypnotist casts some sort of spell over the subject, but in fact no one can be hypnotized against his will and indeed the state represents the ultimate in self-direction. A mild hypnotic state is scarcely discernible from a simple state of relaxed alertness; however, many people are capable of achieving a level of awareness distinctively different from ordinary waking consciousness. The physiological correlates of this state have not been ascertained, but it is characterized at the core by heightened suggestibility. It is a state of highly focused attention, where peripheral distractions are completely blocked out, and where inner events seem as real as only external reality ordinarily seems. In this state, people who are highly susceptible to hypnosis can do extraordinary things at will, such as block out pain or retrieve memories that have been otherwise inaccessible.

Because people are so suggestible under hypnosis, and because such powerful emotions can be released with the procedure, experts in hypnosis believe that it should only be conducted by persons with broad training in psychology. They also contend that, because memory is so malleable, no information elicited through hypnosis should be admitted in court unless it has been independently corroborated.

This puts academics at serious odds with many law enforcement officials, whose attitude is personified by Martin Reiser, a clinical psychologist who heads the Los Angeles Police Department's behavioral sciences services. Reiser, who may be the country's leading exponent of forensic use of hypnosis, thinks the LAPD is way ahead of most of the rest of the country because it has detectives specially trained in "investigative hypnosis." Reiser contends that this is a

0036-8075/80/0627-1443$00.50/0