12-30-09

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 60251
18 December 2009

Mr. John L. Young
251 West 89th Street
New York, NY 10024-1739

Dear Mr. Young:

This is an initial response to your Freedom of Information Act (FOIA) request submitted via the Internet on 25 November 2009, which was received by this office on 27 November 2009, for all documents pertaining to a letter written by Joseph A. Meyer to the IEEE in August 1977 concerning possible ITAR violations of cryptography research exported to countries outside the United States unless by export license, including the actual letter. Your request has been assigned Case Number 60251. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you.

For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. As such, you are allowed 2 hours of search and the duplication of 100 pages at no cost. There are no assessable fees for this request.

Your request is being processed under the FOIA and some of the documents you requested are enclosed. Certain information, however, has been deleted from the enclosures and one document (29 pages) has been withheld in its entirety. Also, after a reasonable search the actual letter written by Joseph A. Meyer was not located.

Some of the information deleted from the enclosures, as well as that in the fully denied document, was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET or SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national

security. The information is exempt from automatic declassification in accordance with Section 3.3(b)(3) and (8) of E.O. 12958, as amended. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). Regarding the fully denied document, we are not authorized to release Senate documents without the approval of the U.S. Senate. We coordinated the release of this document responsive to your request with the Senate Select Committee on Intelligence, and they asked that we withhold the document.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities, as well as the names of NSA/CSS employees. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798 and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. The fact that we were unable to locate one record responsive to your request, the denial of information in the enclosures, and the denial of one document in full, may be considered by you to be adverse determinations. You are hereby advised of this Agency's appeal procedures. Any person notified of an adverse determination may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the adverse determination. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which you believe release of the information is required and/or the grounds upon which you believe this Agency maintains the unlocated record. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

The remaining material responsive to your request is not voluminous or complex, and your request has been placed in the first-in, first-out processing queue for Non-Personal Easy cases. Because there are several cases ahead of yours in that queue, however, we are unable to finalize your request within 20 days. We appreciate your patience with our efforts to treat all requesters fairly by responding to each on a "first-in, first-out" basis.

FOIA Case: 60251

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (DJP4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s

clearer, but even in 1917 the light...

(U) PUBLIC CRYPTOGRAPHY

(U) Modern cryptography has, since its earliest days, been associated with governments. Amateurs there were, like Edgar Allan Poe, who dabbled in the art, and it has held a certain public fascination from the earliest days. But the discipline requires resources, and only governments could marshal the resources necessary to do the job seriously. By the end of World War II, American cryptology had become inextricably intertwined with the Army and Navy's codebreaking efforts at Arlington Hall and Nebraska Avenue. But this picture would begin changing soon after the war.

(U) Modern *public* cryptography originated with a Bell Laboratories scientist, Claude Shannon, whose mathematics research led him to develop a new branch of mathematics called information theory. A 1948 paper by Shannon brought the new discipline into the

public domain, and from that time on, cryptography became a recognized academic pursuit.[119]

(U) Public cryptography had no market in those days. So when IBM researcher Horst Feistel developed a line of key generators to be embedded in IBM computers, called Lucifer, there was no immediate use for it. But in 1971 Lloyd's Bank of London contacted IBM to ask about the possibility of securing transactions from a cash dispensing terminal. Feistal sent Lucifer to Lloyd's. IBM then formed a group, headed by Walter Tuchman, to develop the idea of encrypting banking transactions.

~~(FOUO)~~ While IBM was developing a market for public cryptography, computers were becoming more common within the government. The 1965 Brooks Act gave the National Bureau of Standards (NBS) authority to establish standards for the purchase and use of computers by the federal government. Three years later, Dr. Ruth Davis at NBS began to look into the issue of encrypting government computer transactions and concluded that it was necessary to develop a government-wide encryption standard. She went to NSA for help. NBS, it was decided, would use the *Federal Register* to solicit the commercial sector for an encryption algorithm. NSA would evaluate the quality,

~~(FOUO)~~ In 1973 NBS solicited private industry for a data encryption standard (DES). The first offerings were disappointing, so NSA began working on its own algorithm. Then Howard Rosenblum, deputy director for research and engineering, discovered that Walter Tuchman of IBM was working on a modification to Lucifer for general use.

~~(S-CCO)~~ The decision to get involved with NBS was hardly unanimous. From the SIGINT standpoint, a competent industry standard could spread into undesirable areas, like Third World government communications, narcotics traffickers, and international terrorism targets.

This argued the opposite case – that, as Frank Rowlett had contended since World War II, in the long run it was more important to secure one's own communications than to exploit those of the enemy.[121]

(b)(3)-P.L. 86-36

~~(FOUO)~~ Once that decision had been made, the debate turned to the issue of minimizing the damage.

NSA worked closely with IBM to strengthen the algorithm against all except brute force attacks and to strengthen substitution tables, called S-boxes. Conversely, NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits. Ultimately, they compromised on a 56-bit key.[122]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~(FOUO)~~ The relationship between NSA and NBS was very close. NSA scientists working the problem crossed back and forth between the two agencies, and NSA unquestionably exercised an influential role in the algorithm. Thus, when DES became official in July 1977, a debate erupted in the academic community over the security of the standard. Scientists charged that NSA had secretly pressured NBS into adopting a nonsecure algorithm. Not only did they contend that the key length was to NSA's liking, they also alleged that the Agency had built a "trap door" into the system that would allow cryptographers at Fort Meade to read it at will. In 1976 David Kahn, the leading non-governmental authority on cryptography, lent academic support to this view. Kahn's allegations were repeated by writers and scientists worldwide. The issue became so charged that a Senate committee in 1977 looked into the allegations. The hearings resulted in a "clean bill of health" for NSA, but it hardly quieted the academic uproar.[123]

(U) To calm the waters, NBS called a conference in August 1976. It solved nothing. Leading academic figures contended that the DES algorithm was so weak that it could be solved with fairly modest resources (on the order of $9 million), while defenders pronounced it secure against virtually any attack feasible at the time. National Bureau of Standards ultimately promised that the DES algorithm would be reevaluated every five years.[124]

(U) The problem was, in large part, one of timing. During the Church and Pike Committee hearings, NSA had been tarred with the same brush that smeared CIA and FBI, and the exculpatory conclusions of the Church Committee were lost in a sea of fine print. What the public remembered were the sensational allegations of journalist Tad Szulc and the finger-pointing of former cryptologist Winslow Peck. Whether NSA was an apolitical collector of foreign intelligence information or truly a governmental "Big Brother" had not yet been adjudicated in the public mind. The concern for individual privacy, largely an outgrowth of the Watergate period, exercised an important sway on the American public, and even Walter Mondale, with years of experience watching over intelligence agencies from his Senate perch, was consumed by this issue when he was Carter's vice president. Any endeavor that would make NSA out as an inspector of private American communications would play negatively. The DES controversy was one of those issues.

(U) In 1976 a related chain of events began which was to flow together with the DES controversy. In that year Martin Hellman of Stanford, one of the world's leading practitioners of the cryptographic arts, and his graduate student, Whitfield Diffie, published "New Directions in Cryptography" in the November issue of *IEEE Transactions on Information Theory*. It contained the first public exposition of what was to become known as public key cryptography. In the Hellman-Diffie scheme, it would be possible for individual communicants to have their own private key and to communicate securely with others without a preset key. All that was necessary was to possess a publicly available key and a private key which could be unlocked only with permission. This revolutionary concept freed cryptography from the burdensome periodic exchange of key with a set list of

correspondents and permitted anyone with the same equipment to communicate with complete privacy.[125]

~~(S)~~ This was the public face of the issue. But like public key cryptography itself, it contained a private story that was much more complex. Hellman, it turned out, had been one of the leading opponents of DES, for the very reason that he distrusted NSA's hand in the algorithm. He had obtained a National Science Foundation (NSF) grant to work on the project. It turned out that there was no legal prohibition against a governmental entity funding private research into cryptography, despite the possibility that such research would break the governmental monopoly on leading edge techniques. And in fact, Hellman and Diffie had discovered a technique that [redacted] James Ellis had discovered six years previously. NSA regarded the technique as classified; now it was out in the open.[126] (b)(1) (b)(3)-P.L. 86-36

(U) In April 1977 David Boak and Cecil Corry of NSA visited Dr. John Pasta, director of NSF's division of mathematical and computer research, to discuss the issue. Since the early 1970s there had been sporadic contact between NSA and NSF, and NSF had agreed to permit a certain amount of NSA "assistance" on these types of projects, but only to examine grant proposals on their technical merits rather than to institute a formal coordination process. Pasta, believing that academic freedom was at stake, held fast to the NSF position and refused to permit NSA to exercise any sort of control over future grants.[127]

~~(FOUO)~~ The difficulties with NSF did not end with the Hellman imbroglio. In 1977 Ronald Rivest of MIT published an NSF-funded paper expanding the public key cryptography idea. He postulated a method of exchanging public and private keys, protecting the private key based on the known fact that large integers are extremely difficult to factor. The new RSA technique (named after its inventors, Rivest, Shamir, and Adleman) depended on finding very large prime numbers, upwards of 100 digits long, a [redacted] (b)(3)-P.L. 86-36 NSA's problem with it was that it had been discovered within the cryptologic community five years earlier and was still regarded as secret. In fact, NSA had reviewed the Rivest application, but the wording was so general that the Agency did not spot the threat and passed it back to NSF without comment. Since the technique had been jointly funded by NSF and the Office of Naval Research, NSA's new director, Admiral Bobby Inman, visited the director of ONR to secure a commitment that ONR would get NSA's coordination on all such future grant proposals.[128]

~~(S)~~ In 1977, a patent controversy stirred the already-choppy waters. George Davida, a University of Wisconsin professor, applied for a patent on a cryptographic device using advanced mathematics techniques and [redacted] shift registers. The COMSEC organization was unruffled, but DDO, fearing the spread of shift register techniques that would give the SIGINT side problems, recommended a secrecy order, which was duly put in place by the Patent Office. The inevitable public debate turned on the issue of academic freedom. NSA answered that if Davida had published the technique in an academic journal he would have been protected, but since he had instead applied for a patent, it (b)(1) (b)(3)-18 USC 798 (b)(3)-P.L. 86-36

appeared that he was in it for the money and thus lacked First Amendment protection. This was incontrovertible logic but bad politics, and once again NSA was forced to back down. The Davida patent was reinstated.[129]

~~(S)~~ Inman, who had just arrived at Fort Meade, clamped down hard on patent review procedures, directing that before secrecy orders could be imposed a senior team headed by the general counsel would review the decision. But the new procedures did not work right away. An independent inventor named Carl Nicolai had invented a "phaserphone," which would encrypt voice communications at an estimated cost of about $100 per commercial model. Again the issue split NSA, with DDO opposing the patent release and COMSEC recommending approval. NSA requested another secrecy order, which the commissioner of patents duly imposed. This generated the predictable storm of academic protest. Davida sought the protection of Warren Magnuson, a friend of the family and a power in the Senate. In the face of the commotion, NSA backed down and the Patent Office lifted the secrecy order.[130]

~~(FOUO)~~ NSA hunted diligently for a way to stop cryptography from going public. One proposal was to use the International Traffic in Arms Regulation (ITAR) to put a stop to the publication of cryptographic material. ITAR, a regulation based on the 1954 Mutual Security Act, was intended to control the export of items that might affect U.S. security by establishing a Munitions List, including SIGINT and COMSEC equipment and cryptographic devices. Companies desiring to export items on the list would have to secure licenses. Within NSA the controversy centered on the academic use of cryptography, absent a specific intention to export the techniques. The legislation granted general exemptions in cases where the information was published and publicly available, but skirted First Amendment issues and focusing on commercial motivations.[131]

(U) This idea was pushed internally by one [redacted] but was just one of several techniques being considered. In July 1977, [redacted] took matters into his own hands. The Institute of Electrical and Electronics Engineers would be holding a symposium on cryptography in Ithaca, New York. Concerned about the potential hemorrhage of cryptographic information, [redacted] sent a letter to E. K. Gannet, staff secretary of the IEEE publications board, pointing out that cryptographic systems were covered by ITAR and contending that prior government approval would be necessary for the publication of many of the papers. The letter raised considerable commotion within IEEE, with scholars racing to secure legal opinions and wondering if the federal government might arrest them and impound the information.[132] (b)(3)-P.L. 86-36

(U) The issue did not stop with IEEE. Someone notified the press, and journalist Deborah Shapley published the entire controversy in an issue of *Science* magazine. Although [redacted] wrote the letter on plain bond paper, Shapley quickly discovered his association, and she claimed that NSA was harassing scientists and impeding research into public cryptography. In her view, the lack of direct traceability constituted smuggling NSA's official view covertly to academia, with plausible deniability. Congressional reaction was swift, and the Senate decided to hold hearings on the issues.[133]

(b)(3)-P.L. 86-36

(U) The [redacted] letter was dispatched, recalled Inman ruefully, on virtually the same date that he became director. It presented him with his first public controversy, only days into his new administration.

~~(FOUO)~~ Inman began cautiously enough with that all-purpose bureaucratic solution, the study committee. That fall and winter he had two groups, NSASAB and a committee of NSA seniors, looking at public cryptography and proposing options. To this extremely complex issue the board of seniors proposed three alternatives:

a. Do nothing. This school of thought, championed by G Group, held that any public discussion would heighten awareness of cryptographic problems and could lead to nations buying more secure crypto devices. This threat was especially acute in the Third World.

b. Seek new legislation to impose additional government controls.

c. Try nonlegislative means such as voluntary commercial and academic compliance.[134]

~~(TS-CCO)~~ The panel concluded that the damage was already so serious that something needed to be done. [redacted] It was essential, then, to slow the rate of academic understanding of these techniques in order for NSA to stay ahead of the game. (There was general recognition that academia could not be stopped, only slowed.)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

(U) Inman first chose the legislative solution. Daniel Silver, the head of NSA's legal team, circulated a draft of a new Cryptologic Information Protection Act. This proposed creating a new entity, the U.S. Cryptologic Board, which could restrict dissemination of sensitive cryptologic material for up to five years and would impose severe penalties (five years in prison, a $10,000 fine) for violation.[135]

(U) But Inman himself recognized the unlikelihood of getting Congress to act. NSA's proposed legislation would run against a strong movement in the opposite direction in both Congress and the White House, where the desire was to unshackle U.S. commerce from any sort of Pentagon-imposed restriction on trade. Even as the NSA seniors were recommending strengthening NSA's control over cryptography, President Carter was signing PD-24. This presidential directive divided cryptography in half. "National security cryptography," that which pertained to the protection of classified and unclassified information relating to national defense, would remain with NSA. But the directive also defined another sort of issue, "national interest" cryptography, which pertained to unclassified information which it was desirable to protect for other reasons (international currency exchange information, for instance). Protecting this type of

information and dealing with the private sector on such protection (for instance, on DES), would become part of the domain of the Commerce Department. The National Telecommunications and Information Administration (NTIA), within Commerce, would be responsible for dealing with the public. NTIA moved promptly to assert its authority in the area of cryptographic export policy and to deal with academia over cryptography. NSA mounted strong opposition to both moves.

~~(FOUO)~~ Daniel Silver's draft legislation was basically dead on arrival, and there is no evidence that it was ever seriously considered. But the war between NSA and Commerce was only beginning. Congressman L. Richardson Preyer, who had taken over Bella Abzug's House Subcommittee on Government Information and Individual Rights, led a series of hearings on NSA's "interference" in academia. Preyer worked under the direction of Congressman Jack Brooks, chairman of the full House Government Operations Committee, who was the most vocal sponsor of Commerce's encroachment on NSA's COMSEC turf. Bolstered by the testimony of David Kahn and George Davida, he was predictably critical of NSA's role in public cryptography. Inman, upset with the draft subcommittee report, went to Congressman Edward Boland, who chaired the HPSCI. Boland, agreeing with Inman's complaint, told Brooks that future matters of this sort, which affected national security and intelligence operations, should be coordinated in advance with his committee. This did not end the sniping between NSA and Brooks, but did give the Agency a powerful ally.[136]

~~(FOUO)~~ Within the administration it was guerrilla warfare. The Carter people came to town temperamentally allied with Brooks and Preyer. Their bent was to loosen Pentagon control of anything, especially anything that might affect individual rights and academic freedom. But Inman was a tough infighter and got the Department of Defense to line up behind NSA's position in opposition to NTIA. Through four years of Carter, the matter dogged the White House and frustrated compromise between the Commerce position and the Pentagon determination to gain back its authority. By the time Dr. Frank Press, Carter's advisor on technology policy, was ready to adjudicate the dispute, the 1980 elections were upon the administration, and the solution was deferred to the incoming Reagan people. In the meantime, Inman had succeeded in dividing Congress and securing allies in the fight.[137]

(U) Inman was convinced from the start that the legislative approach, even if successful, would have to be supplemented by some sort of jawboning with academia. Early in his administration, he decided to visit Berkeley, a center of opposition to any sort of government intervention, and a hotbed of raw suspicion since the early days of the Vietnam War. He found himself in a room with antiestablishment faculty members, and "for an hour it was a dialogue of the deaf." Then the vice chancellor of the University of California, Michael Heyman, spoke up. Just suppose, he said, the admiral is telling the truth and that national security is being jeopardized. How would you address the issue? Instantly the atmosphere changed, and the two sides (Inman on one side, the entire faculty on the other) began a rational discussion of compromises. This convinced him that he was on the right track, and he pursued this opening to the public.[138]

(U) Inman followed this with a visit to Richard Atkinson, head of the National Science Foundation, to discuss the ideas that had emerged at Berkeley. The faculty had expressed a desire to get an "honest broker," one that both sides trusted, to sort through the issues and get to a compromise. Atkinson suggested that they approach the American Council on Education (ACE), and agreed that if ACE would agree to sponsor the effort, the National Science Foundation would fund it.[139]

(U) This presented NSA with a historic opportunity to engage in a rational debate with the private sector, and it drove Inman to bring the issue to the attention of the American public. His forum was the annual meeting of the Armed Forces Communications Electronics Association in January 1979. It was the first public speech by an NSA director, and as Inman said at the outset, it was "a significant break with NSA tradition and policy." He then laid out the conflicting interests – academic freedom versus national security. He advocated a problem-solving dialogue, but also acknowledged that the government might on occasion have to impose restrictions on extremely sensitive technology to protect national security. "I believe that there are serious dangers to our broad national interests associated with uncontrolled dissemination of cryptologic information within the United States. It should be obvious that the National Security Agency would not continue to be in the signals intelligence business if it did not at least occasionally enjoy some cryptanalytic successes." On the other hand, the government might have to permit the free exchange of technology, taking action in only the most difficult cases. The important thing, he stressed, was to talk through these issues so that both sides understood what was at stake and could appreciate the position of the other side. And he articulated the long-range importance of the problem: "Ultimately these concerns are not those merely of a single government agency, NSA. They are of vital interest to every citizen of the United States, since they bear vitally on our national defense and the successful conduct of our foreign policy." [140]

(U) The public opening was followed by a series of meetings, sponsored by ACE, to devise a forum to begin the dialogue. Some members (most notedly George Davida) held out for a complete absence of any controls on academia, but the majority concluded that controls would be necessary when national security was involved. What emerged was a procedure for prior restraint, involving a board of five members, a minority of whom would be from NSA, to review publication proposals. Submissions would be voluntary, and the area of examination would be very limited. The proposal passed with the unlikely Yes vote of Martin Hellman, who had earlier been subjected to some private jawboning by Inman. He, along with others in academia, had come to believe that there was, indeed, a legitimate national security interest in what they were doing.[141]

(U) Prepublication review turned out to be less of a real than an imagined threat to First Amendment freedoms. The committee requested very few changes to proposals, and most of those were easily accomplished. In one case, NSA actually aided in lifting a secrecy order placed on a patent application. The submitter, Shamir of RSA fame, thanked NSA for its intervention. At the same time, NSA established its own program to fund research proposals into cryptography. Martin Hellman was one of the first applicants.[142]

(U) As for DES, the controversy quieted for a period of years. DES chips were being manufactured by several firms and had become a profitable business. In 1987, NSA proposed a more sophisticated algorithm, but the banking community, the prime user of DES, had a good deal of money invested in it and asked that no modifications be made for the time. By the early 1990s it had become the most widely used encryption algorithm in the world. Though its export was restricted, it was known to be widely used outside the United States. According to a March 1994 study, there were some 1,952 products developed and distributed in thirty-three countries.[143]

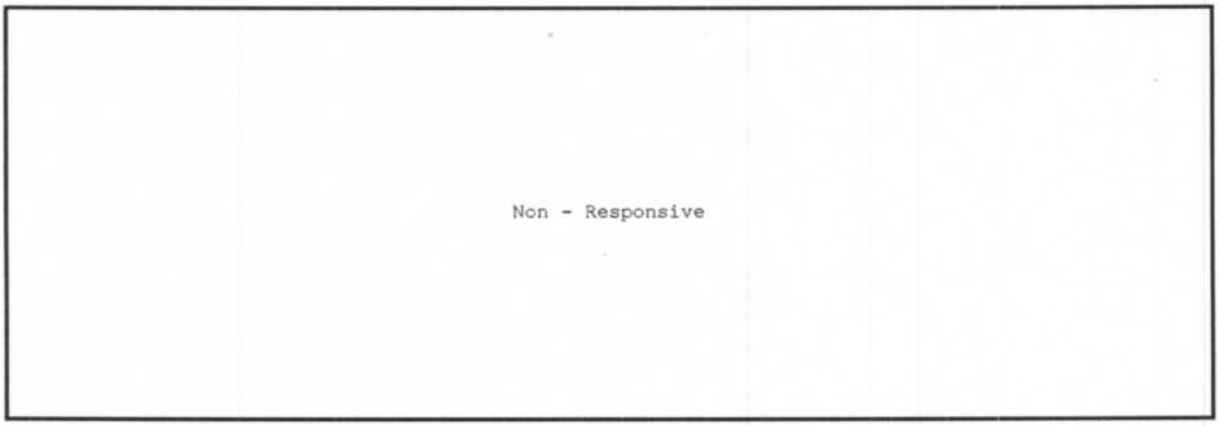
Notes

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive



119. (U) DDIR files, 96026, Box 4, Drake Notebook, Proto Paper.

120. (U) Ibid; draft history of COMPUSEC, in CCH files; "NSA Comes Out of the Closet: The Debate over Public Cryptography in the Inman Era," *Cryptologic Quarterly*, (Spring 1996) 15: 6-7.

121. (U) Ibid.

122. (U) Ibid.

123. (U) DDIR files, 96026, Box 4, Drake Notebook, Proto paper; David Kahn, "Cryptology Goes Public," *Foreign Affairs* (Fall 1979) 147-51 "NSA Comes Out of the Closet," 12-14.

124. (U "NSA Comes Out of the Closet," 8-9.

125. (U "NSA Comes Out of the Closet," 10 *Fifty Years of Mathematical Cryptanalysis* (Fort Meade, Md.: NSA, 1988), 80.

126. (U "NSA Comes Out of the Closet," 10 *Fifty Years of Mathematical Cryptanalysis*, 78.

127. (U "NSA Comes Out of the Closet," 10.

128. (U "NSA Comes Out of the Closet," 10 *Fifty Years of Mathematical Cryptanalysis*, 80.

129. (U) Kahn, "Cryptology Goes Public," 154-55 "NSA Comes Out of the Closet," 16.

130. (U) Kahn, "Cryptology Goes Public," 155 "NSA Comes Out of the Closet," 16.

131. (U "NSA Comes Out of the Closet," 11; DDIR files, 96026, Box 4, Drake Notebook.

132. (U) Kahn, "Cryptology Goes Public," 155-56; "NSA Comes Out of the Closet," 13.

133. (U "NSA Comes Out of the Closet," 12.

134. (U) Ibid., 20-21.

135. (U) Ibid., 25.

136. (U) Ibid., 17-18, 32-35.

137. (U) Ibid.

138. (U) Interview, Norman Boardman, by Robert D. Farley, 17 January 1986, OH 3-86, NSA.

139. (U) Ibid.

140. (U) CCH Series VI.D.2.30.

141. (U "NSA Comes Out of the Closet," 28-31.

(b) (3)-P.L. 86-36

142. (U) Boardman interview; Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM), *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy* (New York: ACM, 1994).

143. (U) Kahn, "Cryptology Goes Public(b)(3)-P.L. 86-36omes Out of the Closet," 13; *Codes, Keys, and Conflicts*, 4-5; Telephone interviev(b)(3)-P.L. 86-36uary 1998.

SCIENCE, VOL. 211, 13 MARCH 1981

MIT Committee Seeks Cryptography Policy

Questions of who should do research on cryptography and how results should be disseminated are the first order of business

Within the next 10 years, networks consisting of tens of thousands of computers will connect businesses, corporations, and banks in giant webs, predicts Michael Dertouzos, director of the Laboratory for Computer Science at the Massachusetts Institute of Technology. But the interconnectedness of these computers, which is their very strength, is also their weakness, he says. Unless steps are taken to assure the privacy of computer data and to assure that computer messages can be "signed," it becomes extraordinarily easy to commit crimes and hard to detect them.

Although a number of computer crimes have been reported, many more are not because banks and corporations do not wish to publicize the weaknesses of their systems. And the crimes that are detected, many experts believe, are only the tip of the iceberg. The FBI, aware of this problem, has mounted a major effort to detect computer crimes in the banking industry.

Dertouzos and others at MIT are extremely concerned about the consequences for individuals and for society if computers continue to be connected, as they are now, according to local decisions by individual entrepreneurs. The security of computer data varies greatly and there is no general assurance that data are safe.

Last fall, MIT formed a committee, headed by Dertouzos and called On the Changing Nature of Information, to look into questions of computer security and other matters arising from the proliferation of computer networks. The committee's members include Francis Low and Walter Rosenblith, the current and past provosts of MIT, and John Deutch, the under secretary of energy in the Carter Administration. They also include a computer scientist and lawyer, and professors of political science, philosophy, and management.

As Dertouzos explains, even if a computer is thought of simply as a filing cabinet, the problem of preventing crime is considerable. The very power of the computer can be used to break the defenses of the installation. It is relatively easy to send computer programs between connected machines and to instruct a program to search for, select, and copy data from anywhere in a network. Then the program can be instructed to remove itself without leaving a trace. By analogy, he says, "Consider a network of filing cabinets, connected by subterranean tunnels. Now imagine that agents can crawl through these tunnels, copy anything they want from any of the files, and leave with no signs of their presence. That is one of the situations we are faced with."

Other issues that will arise as computer networks proliferate, the MIT committee predicts, are questions about what types of data should be stored in computers and for how long, how programs can be protected since they can neither be patented nor effectively copyrighted, the extent to which information should be treated as property, and who is liable if a mistake is made, for example in a medical diagnosis that is assisted by a computer. Although the committee intends eventually to address these questions, its first order of business is to recommend MIT policies for conducting research in cryptography—the principal means by which computer data will be protected, if they are protected at all.

For the past few years, MIT computer scientists and mathematicians have been doing research in cryptography. They have been well aware, however, that the National Security Agency (NSA) considers cryptography research to be potentially threatening to the agency's information-gathering and information-protecting mission. It is not clear whether the NSA has any legal means to prevent the publication of research results it considers damaging. One way it may attempt to do so is through the International Traffic in Arms Regulations (ITAR), which restrict the export of sensitive technical data. But these regulations are vague and difficult to interpret. For example, although, according to the ITAR, publications in international journals are considered to be exports, and although the definitions of technical data in the regulations would seem to include descriptions of computer algorithms, it is not certain whether the ITAR restrict the publication of computer algorithms relating to cryptography. The NSA's counsel claims that the ITAR are enforceable, but the Justice Department says they are unconstitutional.

The NSA has so far been pursuing a voluntary approach to clamping down on the open publication of cryptography research. It has encouraged the American Council on Education (ACE), an organization of university administrators, to establish a Public Cryptography Study Group. The group recently recommended that researchers submit papers on cryptography to the NSA for review before publication (*Science*, 20 February 1981, p. 797).

According to Dertouzos, MIT had let the NSA know that it was interested in participating in the cryptography study group, but it was not invited to send a representative to the group's meeting. Dertouzos says that since it was not announced that observers were welcome, it never occurred to him or others at MIT that they could simply show up and participate in the meetings. "That is not the way we are accustomed to doing things," he remarks. Dertouzos believes that his university had something to contribute to the study group because it has worked out its own arrangement to inform the NSA of MIT research on cryptography—an arrangement that does not involve prior restraints on publications.

MIT first became involved with the NSA in 1977 when faculty members Ronald Rivest, Adi Shamir, and Leonard Adleman published a paper describing a new coding scheme. This was the first of a wave of papers on such schemes which, unlike traditional codes, allow for computerized "signatures" of messages. Rivest, Shamir, and Adleman had planned to present their work at a symposium on cryptology at a meeting of the Institute of Electrical and Electronic Engineers (IEEE). They were deterred, however, when an NSA employee, acting on his own, wrote a letter to the IEEE warning that the ITAR might prohibit such a symposium and also might prohibit the distribution of papers on cryptography (*Science*, 30 September 1977, p. 1345). The symposium was held anyway and, on the advice of the MIT lawyers, the MIT group presented its paper. But Rivest said his group still had "some residual uncertainty" about the legality of its presentation.

Dertouzos, after consulting with MIT lawyers, stopped publication of the Rivest, Shamir, and Adleman paper until the legal situation could be cleared up. Then Dertouzos and Rivest visited the NSA to learn of the agency's concerns. Their discussion led Dertouzos to propose that MIT keep the NSA informed of its research on cryptography by sending the agency prepublication copies of potentially sensitive papers at the same time as the papers are sent to professional colleagues. But, says Dertouzos, "We do *not* say that we will accept a review or decision by the NSA. We send them our papers simply to alert them. We consider our system to be substantially different from the one the ACE cryptography study group recommended." So far the MIT system has worked well. "The NSA has sent back only praise for our work," says Dertouzos.

The legal consequences of publishing results of cryptography research continue to be murky, however. Although MIT decided to resume distributing the 1977 paper by Rivest, Shamir, and Adleman shortly after Dertouzos and Rivest visited the NSA, the university remains concerned about the legal issues in the open publication and distribution of such results. The MIT committee on the changing nature of information has retained lawyers in Boston and in Washington to interpret regulations that may bear on these issues. The committee also is considering various scenarios such as what could happen if an MIT graduate student made a major discovery that not only revealed how to break certain codes but that also had important practical consequences in scheduling theory. What if the student were a foreigner? By this summer, the committee hopes to have developed a set of policies that should clarify how MIT researchers should disseminate the results of their work on cryptography.

The MIT committee members are extremely disturbed by the recommendations of the Public Cryptography Study Group. "There is an aura emerging that the universities have agreed to this sort of review," says Dertouzos. "This university certainly has not. It has neither been consulted nor represented by the ACE."

Cont

MIT provost Low also expresses concerns about the public cryptography study group. Prior restraints, even voluntary ones, "pose serious problems for the universities and for society in general," he says. "Many will not do cryptography research and those who do will do so under conditions where they are less productive and their work is less widely disseminated. The prior restraints will impede what we do and will not succeed in keeping secrets," he says.

Asked whether he could conceive of any situation in which cryptographic research by U.S. scientists should not be published, Low first says that he is not an expert in the area but then remarks that this research is international in scope and that many seminal ideas have already been published. He continues, "My impression of cryptography is that the cat is already out of the bag. All you would gain by secrecy is 1 or 2 years of lead time in proliferation. What you would lose is commercial dissemination in a society that is rapidly becoming more computerized."

—GINA BARI KOLATA