"Cryptography in the Open"
Henry Corrigan-Gibbs

1 The Controversial Symposium

The International Symposium on Information Theory is not known for its racy content or politically charged presentations, but the Symposium in 1977 was a special case. In addition to the relatively common fare on information theory, with titles like "Distribution-Free Inequalities for the Deleted and Holdout Error Estimates," the conference featured presentations by a group of researchers who had drawn the ire of the National Security Agency and the attention of the national press.[1]

The researchers in question were Martin Hellman, an associate professor of electrical engineering at Stanford, and his students, Steve Pohlig and Ralph Merkle. Hellman had caused a stir in the world of electrical engineering and computer science just a year before by publishing a paper, "New Directions in Cryptography," with his student Whitfield Diffie.[2]

The paper was extraordinarily influential and far-sighted—it introduced the principles which form the basis for all of modern cryptography. "The reception [to the paper] from the open community, you know the non-military community," Hellman recalled in a 2004 interview, "was ecstatic."[3] In contrast, "[t]he reception from NSA was apoplectic."[4]

The fact that Hellman and his students were challenging the U.S. government's long-standing domestic monopoly on cryptography deeply annoyed many in the intelligence community.[5] The National Security Agency acknowledged that Diffie and Hellman had come up with their ideas without access to classified materials. Even so, in the words of a recently declassified internal NSA history, "NSA regarded the [Diffie-Hellman] technique as classified. Now it was out in the open."[6]

To make matters worse, Hellman and his colleagues were continuing to spill their powerful cryptographic techniques into the public domain at a breakneck pace. At the International Symposium on Information Theory, to be held on October 10, 1977 at Cornell University, Hellman,

1. Luc Devroye and T.J. Wagner, "Distribution-free inequalities for the deleted and holdout error estimates," *Information Theory, IEEE Transactions on* 25, no. 2 (1979): 202–207.

2. Whitfield Diffie and Martin E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on* 22, no. 6 (1976): 644–654.

3. Jeffrey R. Yost, *Oral history interview of Martin Hellman in Palo Alto, California*, http://purl.umn.edu/107353, OH 375, Charles Babbage Institute, University of Minnesota, Minneapolis, November 2004, 30.

4. Yost, 30.

5. *Martin Edward Hellman Papers*, SC1176, Dept. of Special Collections and University Archives, Stanford University Libraries, Stanford, California, NSA Documents, 233.

6. *Martin Edward Hellman Papers*, NSA Documents, 234.

Pohlig, Merkle, and others were to present their most recent research on algorithms for solving a number of central problems in cryptography.[7]

A Concerned Citizen

The tension between Hellman and the NSA only got worse in the months leading up to the 1977 Symposium. In July of that year, someone named J. A. Meyer sent a shrill letter to the Institute of Electrical and Electronics Engineers (IEEE). The IEEE was the professional organization which published Hellman's papers and which was organizing the upcoming symposium.

Meyer's letter warned that the IEEE might be violating a number of federal statues by publishing the recent research on cryptography.[8] The letter began:

> I have noticed in the past months that various IEEE Groups have been publishing and exporting technical articles on *encryption and cryptology*—a technical field which is covered by Federal Regulations, viz: ITAR (International Traffic in Arms Regulations, *22 CFR 121-128*).[9] [Emphasis in original.]

Meyer's letter asserted that the IEEE and the authors of the relevant papers might be subject to prosecution under federal laws prohibiting arms trafficking laws, communication of atomic secrets, and disclosure of classified information.

Without naming Hellman or his co-authors directly, Meyer referred specifically to the issues of IEEE *Computer* magazine and the IEEE *Transactions on Information Theory* in which Hellman's articles appeared. Concluding his remarks, Meyer warned that "these modern weapons technologies, uncontrollably disseminated, could have more than academic effect."[10]

Meyer's letter caused a ruckus in the academic community and the popular press for two reasons.[11] First, Meyer's letter suggested that merely publishing a scientific paper on cryptography would be the legal equivalent of exporting nuclear weapons to a foreign country. If Meyer's interpretation of the law was correct, it seemed to place severe restrictions on researchers' freedom to publish. Second, and more surprising, was the discovery by Deborah Shapley and Gina Kolata of *Science* magazine that Meyer was an employee of the National Security Agency.[12]

7. Deborah Shapley and Gina Bari Kolata, "Cryptology: scientists puzzle over threat to open research, publication," *Science* 197, no. 4311 (September 1977): 1345–9.
8. *Martin Edward Hellman Papers*, Meyer Letter.
9. *Martin Edward Hellman Papers*, Meyer Letter.
10. *Martin Edward Hellman Papers*, Meyer Letter.
11. Malcolm W. Browne, "Harassment Alleged Over Code Research," *New York Times*, October 1977, A26.
12. Shapley and Kolata, "Cryptology: scientists puzzle over threat to open research, publication."

The Legal Question

Hellman received a copy of the Meyer letter in his capacity as a member of the Board of Governors of the IEEE Information Theory Group.[13] Recognizing that continuing to publish might put him and his students in legal jeopardy, Hellman sought advice from John Schwartz, the University Counsel at Stanford, in advance of the October 1977 Symposium.[14]

In his memo to Schwartz, Hellman makes a lucid case for the value of public-domain cryptography research. Although Hellman acknowledges that the U.S. government's cryptographic advantage proved enormously useful in fighting World War II, he argues that circumstances had changed since then. In particular, the spread of computer technology into every sector of the U.S. economy meant that poor encryption and authentication systems could put intellectual property, personal privacy, and critical systems at risk:

> [T]here is a commercial need today that did not exist in the 1940's. The growing use of automated information processing equipment poses a real economic and privacy threat. Although it is a remote possibility, the danger of inadvertent police state type surveillance must be considered. From that point of view, inadequate commercial cryptography (which our publications are trying to avoid) poses an internal national security threat.[15]

In the memo, Hellman describes how his earlier attempts to prevent "stepping on [the] toes" of NSA failed when the Agency's staffers would not even disclose which areas of cryptography research Hellman should avoid.

Responding to Hellman a few days later, Schwartz opined that publishing cryptography research would not in itself violate federal law. Schwartz's findings had a strong legal basis. Two systems governed classified information in the United States at the time, and neither of them seemed to prevent the publication of unclassified research on cryptography.

The first classification system, reauthorized in 1972 by Executive Order 11652, covered "National Security Information." The order explicitly specified military plans, intelligence activities, and cryptographic secrets as "National Security Information" which fell within scope of the order.[16] However, the executive order only applied to "official information and material" "[w]ithin the Federal Government" and it said nothing about outside research[17] There was not a strong legal

13. Yost, *Oral history interview of Martin Hellman in Palo Alto, California*, 33.
14. *Martin Edward Hellman Papers*, Memo from Martin E. Hellman to John Schwartz, October 3, 1977.
15. *Martin Edward Hellman Papers*, Memo from Martin E. Hellman to John Schwartz, October 3, 1977.
16. National Research Council, *A Review of the Department of Energy Classification Policy and Practice* (Washington D.C.: National Academy Press, 1995), 23.
17. Richard Nixon, *Executive Order 11652 - Classification and Declassification of National Security Information and Material*, June 1972.

argument that Hellman's research could be suppressed based on a Presidential decree, especially because Hellman and his students derived their ideas from purely unclassified sources.

The second classification system, authorized by the Atomic Energy Act of 1954 (AEA) covered everything relating to the "design, manufacture, or utilization of atomic weapons."[18] This second system was much more aggressive than the one covering National Security Information: the AEA was authorized by an act of Congress, not an executive order, and it applied to non-government actors. Under the Act, research into nuclear weapons systems was "born classified," even if the research took place without "any involvement by government at all."[19] Although the AEA carried the legal force to regulate public research, it had nothing at all to do with cryptographic research. The latest version of the AEA spans 543 pages and contains not one mention of the word "cryptography."[20]

Neither of the country's two classification systems appeared to cover public cryptography research. There was only one other likely legal tool that the Federal Government could use to prevent the publication of the work of Hellman and his students. This tool was the Arms Export Control Act of 1976, which regulated the export of military equipment. Under a generous interpretation of the law, giving a public presentation on cryptographic algorithms could constitute "export" of arms. It was not at all clear, however, that a prosecution under this act would stand up to a legal challenge on First Amendment grounds.[21]

Evaluating the these laws together, Schwartz concluded that Hellman and his students could legally continue to publish. At the same time, Schwartz noted wryly, "at least one contrary view [of the law] exists" (that of Joseph Meyer).[22]

Even if the law favored Hellman's position, it was clear that if the government decided to prosecute Hellman and his students, the situation could become acutely uncomfortable for everyone involved. Hellman later recalled John Schwartz's informal advice: "If you are prosecuted, Stanford will defend you. But if you're found guilty, we can't pay your fine and we can't go to jail for you."[23]

18. National Research Council, *A Review of the Department of Energy Classification Policy and Practice*, 24.
19. National Research Council, 24.
20. United States Congress, *Atomic Energy Act of 1954*, 42 U.S.C. §2011, 1954.
21. Patrick J. Monahan, "Regulation of Technical Data under the Arms Export Control Act of 1976 and the Export Administration Act of 1979: A Matter of Executive Decision, The," *BC Int'l & Comp. L. Rev.* 6 (1983): 169.
22. *Martin Edward Hellman Papers*, Memo from John J. Schwartz to Martin E. Hellman, October 7, 1977.
23. *Martin Edward Hellman Papers*, Hellman Autobiography, Chapter 1.

"The Hell With This"

The Ithaca Symposium began three days after Schwartz offered his legal opinion, and Hellman, Merkle, and Pohlig had to quickly decide whether to proceed with their presentations in spite of the threat of prosecution, fines, and jail time.[24]

Graduate students typically present their own research results at academic conferences. In this case however, Hellman said that Schwartz recommended against having the students present their papers: since the students were not employees of Stanford, it might have been more difficult for the University to justify paying their legal bills. In addition, dealing with a "multi-year court case" would be harder for a young PhD student than for a tenured faculty member.[25] Hellman, the consummate PhD advisor, left the decision up to the students.

Merkle and Pohlig, Hellman recalled, "initially said, 'We need to give the papers, the hell with this.' "[26] After speaking with their families though, the students agreed to let Hellman present on their behalf.

Was Hellman nervous about presenting the papers? Reflecting in 2004 on the episode, Hellman said:

> It's interesting[,] people have asked me and sometimes talked about how courageous I was to do this. And it's one of those things where it's not courage. You're confronted with a situation where it's so clearly right to do it and you find the courage in yourself.[27]

In the end, the Symposium took place without incident. Merkle and Pohlig stood on stage mute while Hellman presented the papers on their behalf.[28] According to *Science*, the fact that the conference went ahead as planned "left little doubt that the work [in cryptography] has been widely circulated."[29] The fact that a group of non-governmental researchers could publicly discuss research on cutting-edge cryptographic algorithms signalled the end of the U.S. government's domestic control of information on cryptography.

2 The View from Fort Meade

Vice Admiral Bobby Ray Inman took over as director of the National Security Agency in the summer of 1977.[30] Inman was an experienced naval intelligence officer with allies in both political

24. Shapley and Kolata, "Cryptology: scientists puzzle over threat to open research, publication."
25. Yost, *Oral history interview of Martin Hellman in Palo Alto, California*, 36.
26. Yost, 36.
27. Yost, 36.
28. Yost, 36.
29. Deborah Shapley, "Cryptography meeting goes smoothly," *Science* 198, no. 4316 (November 1977): 476.
30. Bobby Ray Inman, Interviewed by Henry Corrigan-Gibbs. Telephone interview. May 13, 2014.

parties, and a history of sound judgement. With an unassuming character and roots in Rhonesboro, Texas, one reporter noted that Inman's "name evokes the spirit of a country music ballad more than an espionage thriller."[31]

If Inman's qualifications for the job at NSA were good, his timing was not. Inman had barely warmed his desk chair at NSA when he was thrust into the center of what he described as "a huge media uproar" over the J. A. Meyer letter.[32]

In a recent interview, Inman ruefully recounted his first days in office:

> Well, I relieved General [Lew] Allen as the Director of NSA on 5 July 1977. That day, a long-time NSA employee named Meyer—furious that General Allen hadn't moved to squelch public research on cryptography—had written a letter to the IEEE telling them they were in violation of the law for researching cryptography [...][33]

Although Inman was concerned about the impact that publication of these new cryptographic techniques would have on NSA's foreign eavesdropping capabilities, he was also confused at why academic researchers were interested in cryptography in the first place.

According to Inman, the primary consumers of cryptographic equipment in 1970s were governments. Apart from that, he said, "the only other people early on in the non-governmental sector who were buying encryption to use were the drug dealers."[34] Given that the NSA already had "incredibly able people working on the systems to be used by the U.S. Government" and that the NSA had no interest in protecting the communications of drug dealers, Inman wanted to find out why these young researchers were so focused on cryptography.[35]

So, in the tradition of an intelligence professional, Inman went to gather some information for himself: he set out for California to meet with the faculty members at Berkeley and Stanford who were causing all of the trouble. He discovered that these researchers were designing cryptographic systems to solve an emerging problem—one that was not quite on the NSA's radar yet: the problem of securing the growing number of commercial computer systems which were subject to attack or compromise. Their position, Inman said, was that

> there's a whole new world emerging out there where there's going to need to be cryptography and it's not going to be provided by the government.[36]

31. Philip Taubman, "Nominee for Deputy Director of C.I.A. an Electronic-Age Intelligence Expert," *New York Times*, February 1981,
32. Inman,
33. Inman.
34. Inman.
35. Inman.
36. Inman.

In a recent interview, Martin Hellman recalled the conversation in similar terms:

> I was working on cryptography from an unclassified point of view because I could see—even in the mid-70s—the growing marriage of computers and communication and the need therefore for unclassified knowledge of cryptography.[37]

Inman realized that the California academics saw strong public cryptographic systems as a crucial piece of a functioning technological environment.

At the same time, Inman was not excited about the prospect of high-grade encryption systems being available for purchase, especially abroad. The sale of cryptosystems on the open market would make it easier for foreign diplomats and military officials to encrypt their traffic, and would make it more difficult for NSA to decode these messages. "We were worried that foreign countries would pick up and use cryptography that would make it exceedingly hard to decrypt and read their traffic," Inman said.[38]

Damage Control

The level of public excitement surrounding the recent cryptography work meant that growth in the field of unclassified cryptography was almost inevitable. In August 1977, *Scientific American* had published a description of a new cryptosystem due to Ron Rivest, Adi Shamir, and Leonard Adleman of MIT. The researchers offered to mail a copy of a technical report describing the scheme, now known as the "RSA system," to anyone who would send a self-addressed stamped envelope to MIT. The authors received 7,000 requests.[39]

To reckon with the growing threat of unclassified cryptography, Inman convened an internal panel at NSA to offer suggestions on what to do. The panel's suggestions, according to an internal report, were stark:

> [T]he board of seniors proposed three alternatives:
>
> (a) Do nothing. [. . .]
>
> (b) Seek new legislation to impose additional government controls.
>
> (c) Try nonlegislative means such as voluntary commercial and academic compliance.
>
> The panel concluded that the damage was already so serious that something needed to be done.[40]

37. Martin Hellman, Interviewed by Henry Corrigan-Gibbs. In-person interview. May 6, 2014.
38. Inman,
39. Steven Levy, *Crypto* (Allen Lane, 2000), 104-5,114.
40. *Martin Edward Hellman Papers*, NSA Documents, 236.

The declassified NSA history and Hellman's recollection both suggest that Inman first tried to get a law drafted that would restrict cryptographic research along the lines of the Atomic Energy Act.[41] For political reasons, though, the proposed bill was "dead on arrival.".[42] Even if Inman could get a bill through Congress, Hellman said that First Amendment would make it difficult to prevent researchers from speaking about their work: "[T]hey may not publish their papers but they'll give 100 talks before they submit it for publication."[43]

As a sort of last-ditch effort at compromise, Inman organized a voluntary system of pre-publication review for cryptography research papers.[44] A number of other scientific journals have attempted a similar system of pre-publication review in recent years. "That's really the best anyone has been able to come up with," said Steven Aftergood, an expert on government secrecy at the Federation of American Scientists.[45]

The pre-publication review process never gained much traction with cryptography researchers and it eventually "fell apart" completely "because of the explosion of the digital revolution and the volumes of uses" for cryptography[46] As the world underwent a digital revolution, there was an accompanying "revolution in cryptography," just as Whitfield Diffie and Martin Hellman had predicted in 1976.[47]

3 Aftermath

It is tempting to view the outcome of the conflict between the Stanford researchers and the NSA as an unequivocal victory for freedom of speech and as the beginning of the democratization of the tools of cryptography. There is a grain of truth in this characterization, but it misses the larger effect that the run-in over the Information Theory Symposium had on the academic cryptography community and the NSA.

Hellman and other academic researchers realized that they could win debate, as long as it took place in public. Newspapers and scientific journals found it much easier to sympathize with the group of quirky and passionate academics than with a shadowy and stern-faced intelligence agency. The issue of First Amendment rights, Hellman recalled, also gave the press and the researchers a common cause:

41. *Martin Edward Hellman Papers*; Hellman, NSA Documents, 236.
42. *Martin Edward Hellman Papers*, NSA Documents, 236.
43. Hellman,
44. Inman,
45. Steven Aftergood, Interviewed by Henry Corrigan-Gibbs. Phone interview. May 9, 2014.
46. Inman,
47. Diffie and Hellman, "New directions in cryptography."

> Oh, the press. With the freedom of publication issue, the press was all on our side. There were editorials in the *New York Times* and a number of other publications. *Science*, I remember, had covered our work and was very helpful.[48]

From the other side, leaders of the NSA realized that they would have a very difficult time getting public support to suppress what they considered to be dangerous research results. For this reason, the NSA abandoned the pursuit of legislation to regard cryptographic techniques as "born classified."[49]

Realizing that they would be unable to control the publication of non-governmental cryptosystems, leaders of the NSA turned instead to two elements of non-governmental cryptography over which they had near-total control: research funding and national standards.

The Purse Strings

The federal government funds a huge fraction of research which takes place in the U.S.—federal funding accounted for 53% all basic research funding in 2009.[50] By choosing which research projects to fund, the agencies which disperse these research grants exercise control over what sorts of research take place.

Even before the Ithaca Symposium, the NSA reviewed National Science Foundation (NSF) grant applications which might be relevant to signals intelligence or communications security.[51] The purported reason for these reviews was for the NSA to advise the Foundation on the proposals' "technical merits," but the NSA appeared to use this process to exercise control over non-governmental cryptography research.[52]

For instance, NSA reviewed and approved an NSF grant application from Ron Rivest, who later used the NSF funds to develop the enormously influential RSA cryptosystem. The internal history suggests that NSA would have tried to derail Rivest's grant application if the reviewers had understood what Rivest would do with the money. NSA missed this opportunity, the history complains, because the "the wording" of Rivest's proposal "was so general that the Agency did not spot the threat" of the proposed project.[53]

Two years after the Symposium, in 1979, there was another incident in which Leonard Adleman (another member of the RSA triumvirate) applied to NSF for funding and had his application

48. Yost, *Oral history interview of Martin Hellman in Palo Alto, California*, 36.
49. *Martin Edward Hellman Papers*, NSA Documents, 236–7.
50. National Science Board, *Science and Engineering Indicators 2012*, http://www.nsf.gov/statistics/seind12/pdf/c04.pdf, Arlington, Viriginia, 2012, Chapter 4.
51. *Martin Edward Hellman Papers*, NSA Documents, 243.
52. *Martin Edward Hellman Papers*, NSA Documents, 243.
53. *Martin Edward Hellman Papers*, NSA Documents, 243.

forwarded to the NSA.[54] NSA offered to fund the research in place of NSF, but fearing that his work would end up classified, Adleman protested and eventually received an NSF grant.

Even though NSF appears to have maintained some level of independence from NSA's influence, NSA likely has had greater control over other federal funding sources. In particular, the Department of Defense funds research through the Defense Advanced Research Projects Agency, the Office of Naval Research, the Army Research Office, and other offices. After the run-in with the academic cryptography in the late 1970s, Vice Admiral Inman "secure[d] a commitment" that the Office of Naval Research would coordinate its grants with NSA.[55] Since funding agencies often need not explain why they have rejected a particular grant proposal, it is hard to judge the effect that the NSA has had on this process.

By influencing the flow of federal research funds to non-governmental cryptography researchers, the U.S. intelligence community may be able to control the spread of cryptographic secrets without provoking public reproach over government censorship.

Standards

The NSA has a second tool in its efforts to prevent the spread of cryptographic techniques: control over the national processes for standardizing cryptographic algorithms. To make it easier for different commercial computer systems to interoperate, the National Bureau of Standards (NBS, now called NIST) coordinates a semi-public process to design standard cryptographic algorithms.[56]

Although NSA conceded that it could not control the dissemination of non-governmental research results in cryptography, it *could* prevent high-grade cryptography from getting into the federal standards. Vendors would be hesitant to implement algorithms which were not in the NIST standards. Non-standard algorithms would be harder to deploy in practice and would likely see less adoption in the open marketplace.

The first controversy over NSA's hand in these standards erupted in the 1970s when NSA persuaded NBS to weaken the Data Encryption Standard (DES) algorithm.[57] Martin Hellman mounted a vigorous and ultimately unsuccessful public relations campaign to try to improve the strength of the DES algorithm.[58]

At the time, NSA leadership emphatically denied that it had influenced the DES algorithm. In a public speech in 1979 aimed to quell some of controversy, Vice Admiral Bobby Inman asserted:

54. Whitfield Diffie and Susan Landau, *Privacy on the Line* (Cambridge, Massachusetts: The MIT Press, 2007), 71.
55. *Martin Edward Hellman Papers*, NSA Documents, 243.
56. Diffie and Landau, *Privacy on the Line*, 67.
57. Levy, *Crypto*, 60.
58. *Martin Edward Hellman Papers*, Correspondence.

"NSA has been accused of intervening in the development of the DES and of tampering with the standard so as to weaken it cryptographically. This allegation is totally false."[59]

Recently declassified documents reveal that Inman's statements were misleading and factually incorrect. NSA tried to convince IBM (which had originally designed the DES algorithm) to reduce the DES key size "from 64 to 48 bits."[60] Reducing the key size would decrease the cost of certain attacks against the cryptosystem. NSA and IBM eventually compromised, the history says, on using a weakened 56-bit key.

Today, Inman acknowledges that NSA was trying to strike a balance between protecting domestic commercial traffic and protecting NSA's ability to eavesdrop on foreign governments:

> [T]he issue was to try to find a level of cryptography that ensured the privacy of individuals and companies against competitors. Against anyone other than a country with a dedicated effort and capability to break the codes.[61]

NSA's influence over the standards process has been particularly effective at mitigating what NSA perceived as the risks of non-governmental cryptography. By keeping certain cryptosystems out of the NBS/NIST standards, NSA has made its mission of eavesdropping on communications traffic easier.

4 Reflections on Secrecy

There are a few salient questions to consider when looking back at these first conflicts between the intelligence community and the academic researchers in cryptography. A starting point for this analysis, Steven Aftergood says, is to consider "whether in retrospect, [the government's] worst fears were realized."[62]

According to Inman, the uptake of the research community's cryptographic ideas came at a much slower pace than he had expected. As a result, less foreign traffic ended up being encrypted than NSA had projected and the consequences for national security were not as dramatic as he had feared. Essentially, Inman recalled, "there was no demand" for encryption systems outside of governments, even though many high-grade systems eventually became available. "You had a supply but no demand for it."[63] Even those people who tried to use high-grade cryptographic tools,

59. Bobby Ray Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector (1979)," ed. Bruce Schneier and David Banisar (New York: John Wiley & Sons, Inc., 1997), 347–355.
60. *Martin Edward Hellman Papers*, NSA Documents, 232.
61. Inman,
62. Aftergood,
63. Inman,

Hellman said, often make mistakes which render their traffic easy for an intelligence agency to decrypt: "people still make a lot of mistakes: use wrong, bad keys, or whatever else."[64]

A second question to consider is whether Martin Hellman was right to worry that a lack of strong cryptography could become an "economic and privacy threat" in a computerized economy.[65] In an unexpected turn, Admiral Inman is worried as much today about protecting non-governmental computer systems as Martin Hellman was in the 1970s. When asked if he would make the same decisions today about non-governmental cryptography as he did in the 70s, Inman replied

> Rather than being careful to make sure that were[n't] going to damage [our collection capabilities] . . . I would have been interested in how quickly they would have been able to make [cryptosystems] available in a form that would protect proprietary information as well as government information.[66]

The theft of the designs for the F-35 jet, Inman said, demonstrate that weak non-governmental encryption and computer security practices can grievously harm national security.

Even though history has vindicated Martin Hellman, he adamantly refuses to gloat over the uncanny accuracy of his predictions and the far-reaching impact of his technical work. On the contrary, Hellman is still deeply troubled by the way he engaged in the debate with NSA over the publication of his papers and the DES encryption standard.

Rather than trying to understand both sides of the issue and make the "right" decision, Hellman said that, in the heat of the controversy, he listened to his ego instead: "The thought just popped into my head: forget about what's right. Go with this, you've got a tiger by the tail. You'll never have more of an impact on society."[67]

Steven Aftergood says that this sort of self-serving reasoning is a hallmark of debates over secrecy in research:

> If you're a researcher and you've achieved some kind of breakthrough, you're going to want to let people know. So you're not a neutral, impartial, disinterested party. You're an interested party.[68]

It was not until Hellman watched the documentary "Day After Trinity," about the development of the atomic bomb, that he realized how dangerous his decision-making process had been. The moment in the documentary that troubled him the most, he recalled, was when the Manhattan

64. Hellman,
65. *Martin Edward Hellman Papers*, Memo from Martin E. Hellman to John Schwartz, October 3.
66. Inman,
67. Hellman,
68. Aftergood,

Project scientists tried to explain why they continued to work on the bomb after Hitler had been defeated.

> [The scientists] had figured out what they wanted to do and had then come up with a rationalization for doing it, rather that figuring out the right thing to do and doing it whether or not it was what they wanted to do. [...]
>
> I vowed I would never do that again. [...] Thinking it through even now I think I still would have done most of what I did. But it could have been something as bad as inventing nuclear weapons and so I vowed I would never do that again.[69]

Making good decisions in these situations, Aftergood says, requires a large dose of "internal restraint" and a certain "degree of trust" between researchers and government officials, "which is often lacking in practice."[70]

Although Martin Hellman and Bobby Ray Inman forged an unlikely friendship in the wake of their run-in in the late 1970s, trust between the academic cryptography community and the NSA is at its nadir. Inman says of the new director of the NSA: "He has a huge challenge on his plate. How does he... can he, in fact, reestablish a sense of trust?"[71]

Diffie and Hellman's now-legendary key-exchange algorithm has an elegant one-line representation ($K_{ij} = \alpha^{X_i X_j} \bmod q$). In contrast, debates over academic freedom and government secrecy do not lend themselves to such a concise formulation. "It's not a neat simple calculation," Aftergood says. "There are competing interests on all sides, and somehow one just has to muddle through."[72]

Acknowledgements

I would like to thank Steven Aftergood, Martin Hellman, and Bobby Ray Inman for taking the time to share their candid opinions and recollections with me.

69. Hellman,
70. Aftergood,
71. Inman,
72. Aftergood,

References

Aftergood, Steven. Interviewed by Henry Corrigan-Gibbs. Phone interview. May 9, 2014.

Board, National Science. *Science and Engineering Indicators 2012*. http://www.nsf.gov/statistics/seind12/pdf/c04.pdf. Arlington, Viriginia, 2012.

Browne, Malcolm W. "Harassment Alleged Over Code Research." *New York Times*, October 1977, A26.

Congress, United States. *Atomic Energy Act of 1954*. 42 U.S.C. §2011, 1954.

Devroye, Luc, and T.J. Wagner. "Distribution-free inequalities for the deleted and holdout error estimates." *Information Theory, IEEE Transactions on* 25, no. 2 (1979): 202–207.

Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." *Information Theory, IEEE Transactions on* 22, no. 6 (1976): 644–654.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line*. Cambridge, Massachusetts: The MIT Press, 2007.

Hellman, Martin. Interviewed by Henry Corrigan-Gibbs. In-person interview. May 6, 2014.

Inman, Bobby Ray. Interviewed by Henry Corrigan-Gibbs. Telephone interview. May 13, 2014.

———. "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector (1979)," edited by Bruce Schneier and David Banisar, 347–355. New York: John Wiley & Sons, Inc., 1997.

Levy, Steven. *Crypto*. Allen Lane, 2000.

Martin Edward Hellman Papers, SC1176. Dept. of Special Collections and University Archives, Stanford University Libraries, Stanford, California.

Monahan, Patrick J. "Regulation of Technical Data under the Arms Export Control Act of 1976 and the Export Administration Act of 1979: A Matter of Executive Decision, The." *BC Int'l & Comp. L. Rev.* 6 (1983): 169.

National Research Council. *A Review of the Department of Energy Classification Policy and Practice*. Washington D.C.: National Academy Press, 1995.

Nixon, Richard. *Executive Order 11652 - Classification and Declassification of National Security Information and Material*, June 1972.

Shapley, Deborah. "Cryptography meeting goes smoothly." *Science* 198, no. 4316 (November 1977): 476.

Shapley, Deborah, and Gina Bari Kolata. "Cryptology: scientists puzzle over threat to open research, publication." *Science* 197, no. 4311 (September 1977): 1345–9.

Taubman, Philip. "Nominee for Deputy Director of C.I.A. an Electronic-Age Intelligence Expert." *New York Times*, February 1981.

Yost, Jeffrey R. *Oral history interview of Martin Hellman in Palo Alto, California*. http://purl.umn.edu/107353, OH 375. Charles Babbage Institute, University of Minnesota, Minneapolis, November 2004.