KEEPING

BY HENRY CORRIGAN-GIBBS

ILLUSTRATIONS BY BRIAN STAUFFER

SECRETS

Four decades ago, university researchers figured out the key to computer privacy, sparking a battle with the National Security Agency that continues today.

WHAT IF

your research could help solve a looming national problem, but government officials thought publishing it would be tantamount to treason? A Stanford professor and his graduate students found themselves in that situation 37 years ago, when their visionary work on computer privacy issues ran afoul of the National Security Agency. At the time, knowledge of how to encrypt and decrypt information was the domain of government; the NSA feared that making the secrets of cryptography public would severely hamper intelligence operations. But as the researchers saw it, society's growing dependence on computers meant that the private sector would also need effective measures to safeguard information. Both sides' concerns proved prescient; their conflict foreshadowed what would become a universal tug-of-war between privacy-conscious technologists and security-conscious government officials.

A CONTROVERSIAL SYMPOSIUM

The International Symposium on Information Theory is not known for its racy content or politically charged presentations, but the session at Cornell University on October 10, 1977, was a special case. In addition to talks with titles like "Distribution-Free Inequalities for the Deleted and Holdout Error Estimates," the conference featured the work of a group from Stanford that had drawn the ire of the National Security Agency and the attention of the national press. The researchers in question were Martin Hellman, then an associate professor of electrical engineering, and his students Steve Pohlig, MS '75, PhD '78, and Ralph Merkle, PhD '79.

A year earlier, Hellman had published "New Directions in Cryptography" with his student Whitfield Diffie, Gr. '78. The paper introduced the principles that now form the basis for all modern cryptography, and its publication rightfully caused a stir among electrical engineers and computer scientists. As Hellman recalled in a 2004 oral history, the nonmilitary community's reaction to the paper was "ecstatic." In contrast, the "NSA was apoplectic."

The fact that Hellman and his students were challenging the U.S. government's longstanding domestic monopoly on cryptography deeply annoyed many in the intelligence community. The NSA acknowledged that Diffie and Hellman had come up with their ideas without access to classified materials. Even so, in the words of an internal NSA history declassified in 2009 and now held in the Stanford Archives, "NSA regarded the [Diffie-Hellman] technique as classified. Now it was out in the open."

The tension between Hellman and the NSA only worsened in the months leading up to the 1977 symposium. In July, someone named J. A. Meyer sent a shrill letter to the Institute of Electrical and Electronics Engineers, which had published Hellman's papers and was holding the conference. It 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).

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, communication of atomic secrets and disclosure of classified information.

Without naming Hellman or his co-authors, Meyer specified the issues of IEEE's *Transactions on Information Theory* journal and *Computer* magazine in which Hellman's articles appeared. Meyer concluded ominously that "these modern weapons technologies, uncontrollably disseminated, could have more than academic effect."

Meyer's letter alarmed many in the academic community and drew coverage by *Science* and the *New York Times* for two main reasons. First, the 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, Deborah Shapley and Gina Kolata of *Science* magazine discovered that Meyer was an NSA employee.

As soon as Hellman received a copy of the letter, he recognized that continuing to publish might put him and his students in legal jeopardy, so he sought advice from Stanford University counsel John Schwartz.

In his memo to Schwartz, Hellman made a lucid case for the value of public-domain cryptography research. Astutely, Hellman first acknowledged that the U.S. government's tight control over cryptographic techniques proved enormously useful in World War II: Allied forces used confidential cryptographic discoveries to improve their own encryption systems while denying those same cryptographic benefits to Axis powers. Even so, Hellman argued that circumstances had changed.

> [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 initially inadvertent police state type surveillance through computerization must be considered. From that point of view, inadequate commercial cryptogra-

phy (which our publications are trying to avoid) poses an internal national security threat.

In the memo, Hellman described how his earlier attempts to prevent "stepping on [the] toes" of the 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. His findings had a strong legal basis: Two regulations governed classified information in the United States at the time—an executive order and the Atomic Energy Act of 1954—and neither seemed to prevent the publication of unclassified research on cryptography.

There was only one other likely legal tool that the federal government could use to prevent the Stanford group from disseminating their work: 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 clear, however, that a prosecution under this act would stand up to a legal challenge on First Amendment grounds.

Evaluating 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 A. Meyer. Hellman later recalled Schwartz's less-than-comforting 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."

The Cornell symposium was to begin three days after Schwartz offered his legal opinion; 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. Graduate students typically present their own research at academic conferences, but according to Hellman, Schwartz recommended against it in this case. Since the students were not employees of Stanford, it might be more difficult for the university to justify paying their legal bills. Schwartz also reasoned that dealing with a lengthy court case would be harder for a young PhD student than for a tenured faculty member. Hellman left the decision up to the students.

According to Hellman, Merkle and Pohlig at first said, "We need to give the papers, the hell with this." After speaking with their families, though, the students agreed to let Hellman present on their behalf.

In the end, the symposium took place without incident. Merkle and Pohlig stood on stage while Hellman gave the presentation. The fact that the conference went ahead as planned, *Science* observed, "left little doubt that the work [in cryptography] has been widely circulated." That a group of nongovernmental researchers could publicly discuss cutting-edge cryptographic algorithms signaled the end of the U.S. government's domestic control of information on cryptography.

THE VIEW FROM FORT MEADE

Vice Adm. Bobby Ray Inman took over as director of the NSA in the summer of 1977. Inman was an experienced naval intelligence officer with allies in both political parties. If his qualifications for the job were good, his timing was not. He had barely warmed his desk chair when he was thrust into the center of what he recently described as "a huge media uproar" over the J. A. Meyer letter—written the very first day of Inman's tenure.

Although Inman was concerned about the impact that publication of these new cryptographic techniques would have on the NSA's foreign eavesdropping capabilities, he was also puzzled. As he explained, the primary consumers of cryptographic equipment in the 1970s were governments. Apart from that, "the only other people early on . . . who were buying encryption to use were the drug dealers." Since the NSA already had "incredibly able people working on building the systems to be used by the U.S. government" and 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.

In the tradition of intelligence professionals, Inman set out to gather some information for himself. He went to California to meet with faculty members and

SHARING THE STEALTH: Merkle, Hellman and Diffie ended government's monopoly on cryptography.

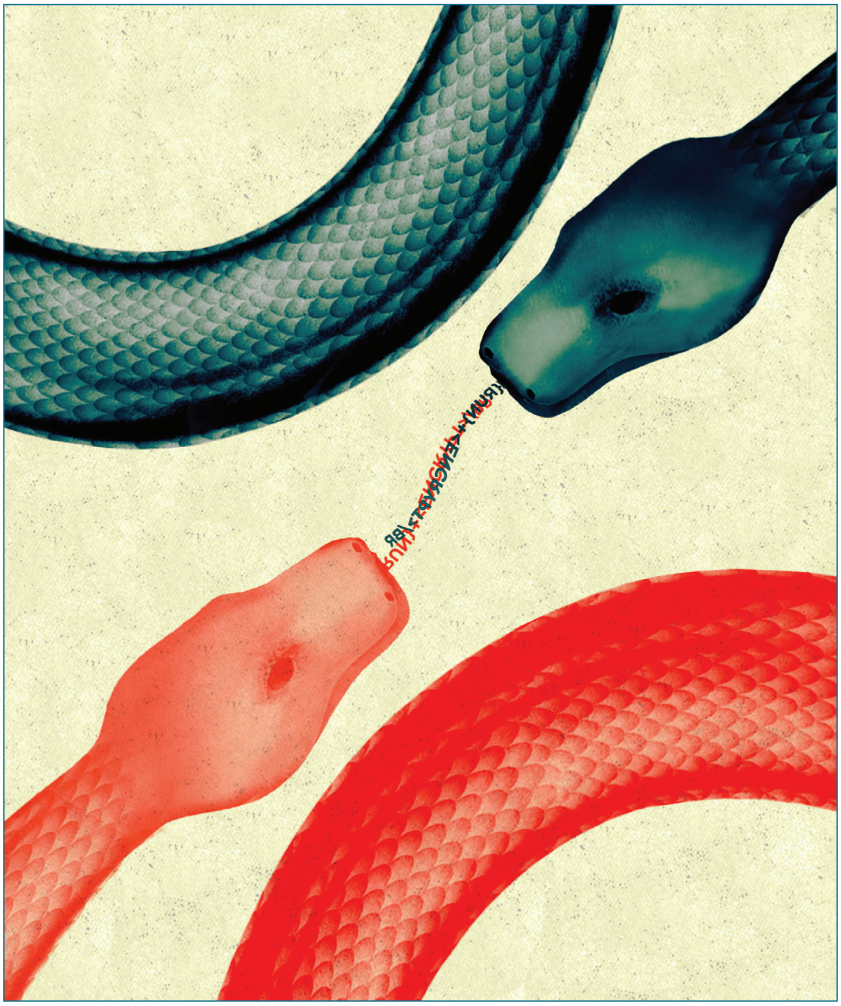
CHUCK PAINTER/STANFORD NEWS SERVICE

industry leaders at Berkeley, Stanford and elsewhere. Inman quickly discovered that the researchers at Stanford were designing cryptographic systems to solve an emerging problem that was not yet on the NSA's radar: securing the growing number of commercial computer systems, which were subject to attack or compromise. The researchers' 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."

Martin Hellman recently recounted their 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." Inman realized that the California academics saw strong public cryptographic systems as a crucial piece of a functioning technological environment.

Still, Inman was not excited about the prospect of high-grade encryption systems being available for purchase, especially abroad. "We were worried that foreign countries would pick up and use cryptography that would make it exceedingly hard to decrypt and read their traffic."

The level of public excitement surrounding the recent cryptography work made growth in the field of unclassified cryptography almost inevitable. In August 1977, *Scientific American* had published a description of the new RSA cryptosystem devised by Ron Rivest, Adi Shamir and Leonard Adleman of MIT. According to Steven Levy's 2001 book *Crypto,* the researchers offered a copy of a technical report describing the scheme to anyone who would send a self-addressed stamped envelope to MIT. The authors received 7,000 requests.



To reckon with the growing threat of unclassified cryptography, Inman convened an internal NSA panel for advice. As recounted in the declassified NSA history, the panel gave Inman three stark choices for how to control the publication of cryptography research:

(a) Do nothing

(b) Seek new legislation to impose additional government controls

(c) Try non-legislative means such as voluntary commercial and academic compliance.

The panel concluded that the damage was already so serious that something needed to be done.

NSA documents and Hellman's recollection both suggest that Inman first tried to get a law drafted to restrict cryptographic research, along the lines of the Atomic Energy Act. For political reasons, the NSA history says, Inman's proposed bill was "dead on arrival."

"Congress [wanted to] unshackle U.S. commerce from any sort of Pentagon-imposed restriction on trade," the history ruefully recounts, and the Carter administration "wanted to loosen Pentagon control of anything, especially anything that might affect individual rights and academic freedom."

Even if Inman could get a bill through Congress, Hellman said, the First Amendment would make it difficult to prevent researchers from speaking publicly about their work. If they didn't publish their papers, "they'll give 100 talks before they submit it for publication."

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

The review process was used for a decade, but Inman recalled that it eventually "fell apart" because of "the explosion of . . . uses" for cryptography. As the world underwent a digital revolution, there was an accompanying "revolution in cryptography," just as Diffie and Hellman had predicted in 1976.

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 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 the run-in had on the academic cryptography community and on the NSA.

Hellman and other academic researchers realized they could win the debate, as long as it took place in public. Newspapers and scientific journals found it much easier to sympathize with a group of quirky and passionate academics than with a shadowy and stern-faced intelligence agency. The issue of First Amendment rights, Hellman recalled in 2004, also gave the press and the researchers a common cause. "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."

From the other side, NSA officials realized they would have a difficult time getting public support to suppress publication of what they considered dangerous research results. They turned instead to two aspects of nongovernmental cryptography over which they had near-total control: research funding and national standards.

As of 2012, the federal government provided 60 percent of U.S. academic research and development funding. By choosing which projects to fund, grant-giving government agencies influence what research takes place.

Even before the 1977 Symposium on Information Theory, the NSA reviewed National Science Foundation grant applications that might be relevant to signals intelligence or communications security. The purported reason for these reviews was for the NSA to advise the NSF on the proposals' "technical merits," but the agency appeared to use this process to exercise control over nongovernmental cryptography research.

For instance, the NSA reviewed and approved an NSF grant application from Ron Rivest. Later, Rivest used the funds to develop the enormously influential RSA cryptosystem, which secures most encrypted Internet traffic today. An internal NSA history suggests that the agency would have tried to derail Rivest's grant application if the reviewers had understood what Rivest would do with the money. The NSA missed this opportunity, the history complains, because the wording of Rivest's proposal "was so general that the Agency did not spot the threat" posed by the project.

In 1979, Leonard Adleman (another member of the RSA triumvirate) applied to the NSF for funding and had his application forwarded to the NSA. According to Whitfield Diffie and Susan Landau's 2007 book, *Privacy on the Line,* the NSA offered to fund the research in lieu of the NSF. Fearing that his work would end up classified, Adleman protested and eventually received an NSF grant.

Even though the NSF appears to have maintained some level of independence from NSA influence, the agency 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 (DARPA), the Office of Naval Research, the Army Research Office and other offices. After the run-in with the academic community in the late 1970s, the NSA history asserts that Vice Adm. Inman "secure[d] a commitment" that the Office of Naval Research would coordinate its grants with the NSA. Since funding agencies often need not explain why they have rejected a particular grant proposal, it is hard to judge the NSA's effect on the grant-making process.

The agency has a second tactic to prevent the spread of cryptographic techniques: keeping high-grade cryptography out of the national standards. To make it easier for different commercial computer systems to interoperate, the National Bureau of Standards (now called NIST) coordinates a semipublic process to design standard cryptographic algorithms. Vendors are hesitant to implement algorithms that are not in the NIST standards: Nonstandard algorithms are harder to deploy in practice and are less likely to see adoption in the open marketplace.

IN THE '70s, ONLY GOVERNMENTS AND DRUG DEALERS WERE BUYING ENCRYPTION. WHY WERE THESE ACADEMICS SO INTERESTED?

The first controversy over the NSA's hand in these standards erupted in the 1970s when it persuaded the bureau to weaken the Data Encryption Standard (DES) algorithm, an NBS-designed cryptosystem widely used by banks, privacy-sensitive businesses and the public. Hellman and his then-student Diffie mounted a vigorous—and ultimately unsuccessful—public relations campaign to try to improve the strength of the DES algorithm.

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

Recently declassified documents reveal that Inman's statements were misleading, if not incorrect. The NSA tried to convince IBM (which had originally designed the DES algorithm) to reduce the DES key size from 64 to 48 bits. Reducing the key size would decrease the cost of certain attacks against the cryptosystem. The NSA and IBM eventually compromised, the history says, on using a weakened 56-bit key.

Today, Inman acknowledges that the NSA was trying to strike a balance between protecting domestic commercial communication and safeguarding its own 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."

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

REFLECTIONS ON SECRECY

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

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 the agency 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." Even those people who try to use high-grade cryptographic tools, Hellman said, often make mistakes that render their traffic easy for an intelligence agency to decrypt: "People still make a lot of mistakes: use wrong, bad keys, or whatever else."

A second question is whether Hellman was right to worry that a lack of strong cryptography could become an "economic and privacy threat" in a computerized economy. In an unexpected turn, today Inman is as worried about protecting nongovernmental computer systems as Hellman was in the 1970s. When asked if he would make the same decisions about nongovernmental cryptography now as he did then, Inman replied, "Rather than being careful to make sure they were[n't] going to damage [our collection capabilities] . . . I would have been interested in how quickly they were going to be able to make [cryptosystems] available in a form that would protect proprietary information as well as government information."

The theft of portions of the designs for the F-35 jet, Inman said, demonstrates that weak nongovernmental encryption and computer security practices can grievously harm national security. Even though history has vindicated Martin Hellman, he adamantly refuses to gloat over the 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 the 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."

'FORGET ABOUT WHAT'S RIGHT. GO WITH THIS... YOU'LL NEVER HAVE MORE OF AN IMPACT ON SOCIETY.'

Aftergood said that this sort of ego-driven 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."

It was not until Hellman watched *Day After Trinity,* a documentary about the development of the atomic bomb, that he realized how dangerous his decision-making process had been. The moment in the film that troubled him most, he recalled, was when the Manhattan Project scientists tried to explain why they continued to work on the bomb after Hitler had been defeated and the threat of a German atom bomb had disappeared. The scientists "had figured out what they wanted to do and had then come up with a rationalization for doing it, rather than 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," Hellman said. "Thinking it through even now, 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."

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

Although Hellman and Inman forged an unlikely friendship in the wake of the conflict in the late 1970s, trust between the academic cryptography community and the NSA is at its nadir. Inman said of the new NSA director, "He has a huge challenge on his plate. How does he . . . can he, in fact, reestablish a sense of trust?"

Diffie and Hellman's now-legendary key-exchange algorithm has an elegant one-line representation. Debates over academic freedom and government secrecy do not lend themselves to such a concise formulation. "It's not a neat, simple calculation," Aftergood said. "There are competing interests on all sides, and somehow one just has to muddle through." ■

HENRY CORRIGAN-GIBBS *is a second-year PhD student in computer science.*