From the Cold War to the Crypto War: Crypto-Advocates, the NSA, and Private Industry in the "New Informational World Order;" 1991-1996

By: Nicholas Shumate

There are strange things done ‘neath the silicon sun,
By techies who moil for gold,
And the network trails have their hacker tales
That would make your blood run cold.

But of all the strange sights o’er the ‘lectronic nights
The strangest I ever did see
Is Phiber, Kapor, and Neidof -and more-
In a room with Ingraham, the Feds, and me.

In the last two years, there’ve been shed bitter tears
Over freedom, computers and crime,
By phone phreaks and hackers, by pirates and crackers
Complaining they shouldn’t do time.

The past had wildcat rules for the data pools;
Then, nary a sheriff we saw.
But the Wild West is done — the settlers have come
And with them, computer law.

Crashes litter the network road.; we’ve viruses, worms, malicious code
Is this freedom you’d spare?
Liberty to compute is not the right to pollute
The datastream we all must share.

It’s been twenty years since the ‘lectronic frontier
Cybernet all our lives interweaves.
With the interconnection comes the right to protection
From predators, vandals and thieves.
Techno-punks, you say, are here to stay.
They’re creative! The economy they’ll save!
But they’re not very nice: selfish — cold as Black Ice
D’you really think they’ll just choose to behave?

The sparks of creation and exploration
Need not conflict with order.
If we teach in school, if we live the ethical rule:
Respect for each other’s border.

Law defends freedom to speak, not to steal or to sneak
Into a private file or a -base.
Law means balancing and sharing, fairness and caring
For individual space.

Is this freedom’s demise? Must users arise
A new Constitution to seek?
No! Ours is doing just fine — it’s been tested by time
Then why else are we here, this week?

As the past parades into future decades,
We’re here now — in real-time — to plan,
To share, to shed light, define the rules and the rights
For the Age of Electronic Man.

Gail Thackeray, 1991

For hundreds of years, encryption has been an asset of the military and the state. At its core, encryption (or the use of cryptography) is simply the scrambling of information so as to render it unreadable by individuals and or systems which lack the requisite knowledge on how to unscramble it. The Caesar cipher, named after Julius Caesar, is one of the most notable and simple examples of encryption whereby letters are systematically substituted for others by sliding down the alphabet. For example, if we applied the Caesar cipher to the term "Cold War" by shifting the alphabet down by four, it would look like "Gsph Aev." Again, this was done by simply shifting the letters down four places in the alphabet, C - G, O - S, L - P, D - H, etc. Although this is an extremely simple example of encryption, the point is that militaries and states throughout history would use these and exponentially more complex forms of cryptography to protect important messages, typically military orders, from prying eyes.

However, taking a look at the digital infrastructure we hold dear today, encryption is commonplace. It is used every time we send a text message, we post to Facebook, we order food from DoorDash, we update our car's firmware, we pay our bills, we send a Snapchat, etc. The point is that it is omnipresent on the Internet and yet is done so seamlessly that many of us don't even realize it is being utilized. This paper explores the crux of this shift, which occurred only in the last half a century.

The end of the Cold War marked a dramatic shift in the American approach to information. As Paul Edwards has shown, the end of the Cold War fundamentally shifted an American closed system of information to one based on open information accessibility. A select few technology enthusiasts rallied together during the first part of the 1990s to discuss how distributed computer networks would deal with this change. At the crux of the debate centered the topic of cryptography.

How did these *crypto-advocates*—computer scientists, scholars, engineers, lawyers, and government agents—understand the need for encryption in the age of the Internet before it went mainstream? What were their main concerns, and how did they reflect the changes occuring in the sociopolitical climate of the early 1990s?

Several scholars, such as Z. Isadora Hellegren and Karina Rider, have illustrated how crypto discourse, which spanned the entirety of the 1990s, was important for understanding Internet freedoms and how it buttressed the Crypto Wars—the series of legal battles which led to the U.S. government relinquishing control over cryptography.[1] In doing so however, scholars have focused more heavily on the cypherpunks, a minor cast of crypto-advocates which mostly consisted of computer engineers such as Eric Huges and Timothy C. May. These individuals,

[1] Karina Rider, "The Privacy Paradox: How Market Privacy Facilitates Government Surveillance," Information, Communication & Society 21, no. 10 (2017): pp. 1369-1385; Z. Isadora Hellegren, "A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom," Internet Histories: Digital Technology, Culture, and Society 1, no. 4 (October 23, 2017): pp. 285-311.

who could better be described as near crypto-anarchists rather than crypto-advocates, were exceptionally fringe outside of the "hacker" community, marked by inflammatory dialogue towards what they perceived as establishment institutions, and almost solely concerned with cryptography from a technical engineering perspective.[2] Because of this, they isolated themselves when compared to their larger crypto-advocate counterpart. By focusing only on cypherpunks, these scholars have contributed to a more fringe understanding of crypto discourse in the early 1990s.

This demographic of crypto-advocates has been covered by communications scholar Fred Turner. In his studies of the WELL (Whole Earth 'Lectronic Link), an online message board, he illustrated how the platform consisted mainly of counterculturalists who emerged out of the desire to escape mainstream society in the 1960s. Many of these counterculturalists lived in or around the Silicon Valley, Stanford University, and the University of California, Berkeley. While they may have had roots on the West Coast, many found themselves distributed across the continental U.S. In order to maintain their sense of identity, they found ways to rally and share ideas that transcended the distance barrier.[3]

Counterculturalists rallied through the Whole Earth Network, a magazine started by Stewart Brand. The Whole Earth Network attempted to bring these individuals together by discussing a lifestyle immersed in nature and technology-oriented advancements of the day. Out of the Whole Earth Network, Stewart Brand launched the WELL using early business conferencing software in an attempt to bring synchronous communication to the Whole Earth community.[4]

However, the State Department considered cryptography a munition, a holdover from the Cold War, and regulated it via the International Traffic in Arms Regulations (ITAR). Crypto-advocates challenged the NSA and the government's control over encryption by focusing on this regulation as their main concern. In essence, developing a form of encryption or using encryption, legally amounted to engaging in arms dealing. The NSA saw issues arising by the late 1970's and early 1980s. It had internal discussions on how best to deal with the rising claims for public encryption, maintain their relevancy in the post-Cold War period, and fulfill their duty to protect national security. These discussions resulted in the Clipper Chip and Data Encryption

[2] Eric Hughes, "A Cypherpunk's Manifesto," Activism.net, March 9, 1993, https://www.activism.net/cypherpunk/manifesto.html); Timothy C. May, "The Crypto Anarchist Manifesto," Activism.net, November 22, 1992, https://www.activism.net/cypherpunk/crypto-anarchy.html); Eric Hughes, "1992-10-05 - A Statement of Purpose," cryptoanarchy.wiki (Cypherpunk Mailing List, October 5, 1992), https://mailing-list-archive.cryptoanarchy.wiki/archive/1992/10/97c0e14e4cbacb0f1cf923b501e37ac37c5bda734512f88e2b11d588b6993e34/)

[3] Turner, *From Counterculture to Cyberculture,* 4-13

[4] Ibid.

Standard (DES), both standardized methods of encryption designed by the government to be susceptible to governmental intrusion.

Crypto-advocates comprised a surprisingly vast institutional demographic, far from the misconception of a few fringe cypherpunks. These individuals consisted of computer science scholars, legal scholars, communications scholars, industry experts, law enforcement and intelligence agency personnel, civil rights and non-profit activists, journalists, authors, and technology enthusiasts. At places such as the Computer, Freedom, and Privacy conference and on the early Internet message board the WELL, these crypto-advocates fought for updated federal and state regulations that would be better equipped to deal with the manifesting computer and Internet cultures. These individuals demanded that fundamental American tenets, such as the First and Fourth Amendments, be applied equally to the digital realm as to the analog and physical realm.

These advocates rallied around public encryption and met with individuals from law enforcement and intelligence agencies at the Computer, Freedom, and Privacy conferences from 1991 to 1996. The CFP conferences, as rendered through the formal dialogue extant in the official proceedings as well as through the informal dialogue between crypto-advocates on the WELL, illuminates how these confrontations, discussions, and connections formed a sort of invaluable contact zone.

There is a distinct lack of information regarding who exactly organized the first CFP conference. It seems to have been a collaborative effort that found fertile ground on the WELL. Some of the earliest extant posts and calls to action were done by Jim Warren, who was a computer security activist and columnist for *MicroTimes,* a San Francisco Bay computer-oriented newspaper.[5] Whether or not he alone spearheaded the CFP conference is unclear. What is clear, however, is that others on the CFP section of the WELL quickly rallied to bring the conference to fruition. The CFP Conference seemed to be a wonderful example of what like-minded individuals could create when they rallied together under a common cause.

At the conferences, individuals from the NSA, FBI, CIA, Congress, federal agencies, and various law enforcement agencies built lasting connections with crypto-advocates. Together, they contributed towards building a better Internet for the 21st century. Although begrudgingly attended by many in the law enforcement and intelligence sectors such as the NSA, these conferences and meetings directly impacted the liberalization of encryption methods. Encryption is foundational for modern communication on the Internet not only as a function of privacy, but also as a function of authentication. Individuals can have some level of trust that they are sending information to their intended recipient and that the information remains private.

[5] Levy, 197.

As the debate between crypto-advocates and law enforcement became more pronounced and garnered mainstream media coverage, Industries and organizations with great amounts of wealth and influence began to plant a larger foothold on the "electronic frontier." This occurred simultaneously as mainstream society began to familiarize itself with the emerging technology. By 1996, these themes had become commonplace at places like the CFP conference and the WELL. At that point, the civilian conglomeration of academics, computer scientists, and technology enthusiasts who first resided and colonized the Net and who formulated the basis of crypto-advocacy found themselves no longer the only residents in the growing Internet metropolis. Industry, which had helped the crypto-advocates legitimize their claims for encryption, proved to be a double-edged sword. Although industry had helped the crypto-advocates legitimize their claims for public encryption, it quickly antiquated the crypto-advocate versus law enforcement paradigm. The first Crypto-War was now over, and it appeared that industry motives would take the foreground by laying the foundation for our informational ethics struggle today.

Counterculturalism and Fear of the State

Historian of the Internet Janet Abbate has illustrated the contention between the civilian and military roots of computers and networking. The Cold War union between academia and the U.S. military dominated networking technology and its associated policy standards. The contentions between the public and military control over the Internet directly impacted crypto-advocates, such as those on the WELL and at the CFP conferences during the 1990s. As the advocates wished to expand civilian control and civilian integration into these emerging systems, they ingrained themselves with academics' demand for civilian access to better encryption methods.

The struggle over public encryption first began in 1970s Cold War America. Whitfiled Diffie and Martin Hellman, two computer professors with Stanford University and future CFP speakers, along with a previously published graduate student, Ralph Merkle, together formulated the basis of public key encryption.[6] Public key encryption not only allowed for feasible encryption over a network of computers, but allowed for users to be authenticated. This is fundamental since the ability to encrypt data and the ability to authenticate that data's source and trajectory, not only laid the basis for crypto-advocate discourse at the end of the Cold War, but more importantly has proved to be foundational to how we currently operate over a distributed computer network—the Internet.

George Davida of the University of Wisconsin was one of the first and most significant academics who fought the NSA's domination over encryption. He did research on cryptography and received a secrecy order in the mail. "It was more or less like a postcard telling me that

[6] Levy, 66-68.

under the penalty of three years in jail and $10,000 fine I am to talk to no one about what I had done in that paper without reference to any classified material." At first, Davida and his graduate research assistant found it hilarious until the gravitas of the situation set in. He came to realize that "privacy is just too important to leave it just to agencies like NSA" who view public "cryptography [as] an evil tool that will only be used by terrorists and drug dealers."[7] Academic computer scientists needed access to these systems to sufficiently continue their research, and by its very nature, academic freedom requires the maintenance of open systems.

The NSA designed and promoted the Clipper Chip in 1993. It encrypted data in such a way that the government could decrypt anything that passed through. The Clinton administration backed the usage of the Clipper Chip as a de jure standard to be used by any U.S. citizen or organization wishing to encrypt any form of information. If the chip was adopted for mass use, government agencies such as the NSA could decrypt any and every form of encryption. One academic at CFP'94 retorted to such proposals with:

> [The Clipper] algorithm is not being made public and yet one of the very basis of scientific research is that the work should be published and then reviewed by the community and approved as the state-of-the-art develops. Yet it seems that the NSA [is] reluctant to do that. There is a certain amount of conjecture that in fact the algorithm contains a deliberately encoded weakness that will allow the NSA, without access to the escrow keys, to be able to intercept communication in their mission to monitor on—shore and offshore—communications. There's a number of us in the scientific community that are greatly concerned that that algorithm is not being made public.[8]

Academics' need for freedom for research purposes combined with crypto-advocates' desire for access to military-grade cryptography. These crypto-advocates wanted access to encryption not as an inherent right of the technology era, but rather because of their counterculturalist distrust of large bureaucracies. In a sense, they wanted public encryption to protect their communications from the prying eyes of the government and in doing so, they instantiated claims of First and Fourth Amendment rights.

The importance of authentication and trust became one of the highlights of crypto-advocates'' claims for democratized encryption. They saw themselves as "pioneers" on the "electronic frontier," and there existed a sense of urgency for reliable systems of communication. Stemming from deeply ingrained governmental distrust came a need for private and reliable

[7] George Davida, "CFP'94 - DATA ENCRYPTION: WHO HOLDS THE KEYS? (Panel)," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 24, 1994), http://cpsr.org/prevsite/conferences/cfp94/encpanel.html/)

[8] Ibid, Unknown Speaker.

communications. These crypto-advocates saw better public encryption as the answer. Bruce Koball stated in 1993 that “the easy availability of secure communications” might lead to more liberal forms of communication. “Not only does your correspondence know that her message will not be intercepted, but also that the intended recipient is who he claims to be!”[9]

Several legislators, such as Senator Patrick Leahy, saw these crypto-advocates as industry experts. As pioneers, crypto-advocates typically referred to themselves as Net experts. They populated the early “electronic frontier,” they helped to establish it, and they were the ones who utilized it. Because of this, they saw themselves as a sort of authority of the Net and any form of Net advocacy ultimately rested on their shoulders. Senate fellow Craig Shiffries stated at the first CFP, CFP’ 91, that a lot of the time, Congress and Congressional staff “don’t have the necessary expertise to work in these areas.” Staff such as that of Senator Leahy were “very active in making sure that people with a broad range of expertise and knowledge are brought into the process in a very consultive way.”[10] Senator Leahy would send representatives, such as Shiffries, “to come to these conferences and to bring back some of the thoughts that were expressed...to see if we can interact with you people and help create sound laws for the future of the electronic frontier.”[11]

Crypto-advocates shared a deep concern about Congressional ignorance of these emerging technologies, and their concern intertwined with the already existing government skepticism of the community. Mary Culnan of Georgetown University and private lawyer Harvey Silverglate reiterated these concerns at CFP’91 when they emphasized that CFP needed a strong and diverse demographic to better inform Congress of something they have little information about. Silvergate mentioned that:

> Unfortunately, few people in the legislative and administrative branches, and even fewer in the judicial branch, understand these technologies and their implications. It is not at all clear that a computer disk will be treated like a filing cabinet for Fourth Amendment (search and seizure, and privacy) purposes. It is not clear that a computer will be given the same First Amendment (free press) protection as a printing press. And it is not a foregone conclusion that computerized bulletin

[9] Bruce Koball, “CFP Conference, Topic 92, Comment 135,” The WELL, October 15, 1993, well.com)

[10] Craig Schriffies (Senate Fellow), “Where Do We Go From Here?,” CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 28, 1991), http://cpsr.org/prevsite/conferences/cfp91/closing.html/)

[11] Ibid.

> boards will be given the First Amendment (free speech) protection of other public communications forums.[12]

He was adamant that unless updated regulations and approaches were integrated with the emerging technology, the lack of public access to encryption would be "a major disaster for the constitutional rights of generations to come."[13] Fears and urgency of this kind was common throughout the early years of the Computer, Freedom, and Privacy Conferences.

In addition, crypto-advocates at the early CFP Conferences debated whether or not the US Constitution should be updated with a 27th Amendment. This hypothetical amendment would strictly guarantee protections on the Internet. Sharon Beckman, another speaker and private lawyer at CFP'91, mentioned that "the constitution, as it exists, even without the need for any constitutional amendment, should be interpreted so that its fundamental underlying values apply in changed circumstances and in the context of new technologies."[14]

As a result, the CFP participants pushed for more open systems at the conferences. Their notions fell into a greater dialogue between privacy and national security. This debate was riddled with Cold War fears of totalitarianism and an embrace of open flow of information and access to technologies such as encryption. John Gilmore of the EFF (Electronic Frontier Foundation) articulated these concerns at CFP'91 when he stated that "this society was built as a free and open society." As he saw it, they built off the American tradition by "making and building this society in such a way—because we believe such a society outperforms closed societies—in quality of life, in liberty, and in the pursuit of happiness."[15] It is no surprise that so shortly after the fall of the Berlin Wall, crypto-advocates were concerned about closed informational practices and totalitarianism.

Participants on the WELL and CFP almost unanimously advocated for open systems. A year later, Gilmore once again condemned NSA practices of controlling cryptography through export controls. Gilmore understood the NSA as an entity that would take advantage of the burgeoning informational economy by throwing around its Cold War armament. "[T]here's an opportunity for the NSA to sort of pull the wool over [smaller institution's] eyes, to say, no, this

[12] Harvey A Silverglate, "The Need to Leap Almost Before You Look: Creating Precedent for Electronic Freedom, Now, or Perhaps Never.," CFP'91 - Index (CPSR: Computer Professionals for Social Responsibility, February 13, 1991), http://cpsr.org/prevsite/conferences/cfp91/silverglate.html/); Mary Culnan, "Where Do We Go From Here?," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 28, 1991), http://cpsr.org/prevsite/conferences/cfp91/closing.html/)

[13] Ibid.

[14] Sharon Beckman, "Law Enforcement & Civil Liberties," CFP'91 - Index (CPSR: Computer Professionals for Social Responsibility, March 27, 1991), http://cpsr.org/prevsite/conferences/cfp91/ddenning.html/)

[15] John Gilmore, "Privacy, Technology, and the Open Society," CFP'91 - Index (CPSR: Computer Professionals for Social Responsibility, 1991), http://cpsr.org/prevsite/conferences/cfp91/gilmore.html/)

is how it has to be, we can't let you get encryption any stronger than this, and that's just the way it is." He struck directly at the concerns of many NSA officials, which will be detailed later, who worried about the NSA budget outside of the Cold War era. "[T]here's been a lot of progress with proposals to cut the military budget, to shrink the black budget, and to stop pretending that we're in a cold war."[16]

Steven Cisler, an Apple Inc. librarian, was one of the most active reporters besides the chairman, Bruce Koball, of CFP activities on the WELL. His interests in broadening information systems and library sciences meshed well with his fellow crypto-advocates. He spoke highly of a speaker who did not consider crypto-advocates "prisoners of geography"; rather, they were liberated by the interconnectedness of the Net. Their "academic interests [could be] shared by the enabling technologies computers...openness, freedom, inclusiveness will help us make a society that will please our children and grandchildren."[17]

Although initially, cryptography and openness may seem to be at odds, from the context of distributed computer systems, they are actually one and the same. As these crypto-advocates saw it, cryptography protected the free flow of information on the Net. Beyond authentication purposes, it allowed individuals to build a network of trust, which allowed for a spectrum of possibilities. Cryptography quickly became the power to associate and communicate. Open information- and crypto-advocates were concerned with liberating that power from the government in the post-Cold War world. Bruce Sterling articulated this quite well in 1993:

> Cryptography is a very hot issue in electronic civil liberties circles at the moment. After years of the deepest, darkest, never-say-anything, military spook obscurity, cryptography is out of the closet and openly flaunting itself in the street. Cryptography is attracting serious press coverage. The federal administration has offered its own cryptographic cure-all, the Clipper Chip. Cryptography is being discussed openly and publicly, and practiced openly and publicly. It is passing from the hands of giant secretive bureacracies [sic],]to the desktop of the individual. Public-key cryptography, in particular, is a strange and novel form of cryptography which has some very powerful collateral applications and possibilities, which can only be described as bizarre, and possibly revolutionary. Cryptography is happening, and happening now.[18]

[16] John Gilmore, "CFP'92 - Who Holds the Keys?," CFP'92 - Index of Papers (CPSR: Computer Professionals for Social Responsibility, March 20, 1992), http://cpsr.org/prevsite/conferences/cfp92/denning.html/)

[17] Steven Cissler, "CFP Conference, Topic 72, Comment 11," The WELL, April 9, 1992, well.com)

[18] Bruce Sterling, "CFP Conference, Topic 92, Comment 22," The WELL, September 22, 1993, well.com)

This contention with the government over individual liberty and regulation came down to a very similar issue already taken up by these crypto-advocate counterculturalists.

Discussion of the right to public encryption often dabbled in a discussion of drug use. Law enforcement and intelligence communities would later take this notion and use it as an example of the need for stricter regulation. In the 1960s, counterculturalists made a case for the right of individuals to partake in drugs like LSD. Again, in 1993, Bruce Sterling made the connection between LSD and cryptography. Although he readily admitted it would never be legal he understood that whereas LSD never "really offered many solid benefits," the benefits of cryptography were infinite.[19] For better or for worse, the linkage between the counterculture movement in the 60s was directly linked to the public encryption movement in the 90s.

One participant at CFP'94 who considered themselves a "fossil from the 60s," Efrem Lipkin went on to describe how their parents had to deal with the House Un-American Activities Committee (HUAC) during their lifetime and how Efrem had fought for civil rights in the 1960s. He mentioned how he "had this surreal experience of" a government agent attempting to "plant a copy of the Daily Worker on" them.[20] Efrem understood that the real privacy protection they needed was from the government, not industry. Their governmental skepticism, at least from their experiences, was well justified and many other such crypto-advocates had similar encounters to share.

Often, the counterculturalists who formulated the foundation of crypto-advocacy also took part in the anti-government movements during the 1960s. Their governmental skepticism was deeply ingrained and already active in such older battlegrounds as with LSD. These academics' and activists' claims of libertarian control over emerging communications networks not only placed them at an advantage on the Net, but also situated them perfectly to advocate for open systems and privacy as epitomized by cryptography. Andrew Brown, a WELL member and journalist who wrote in the Independent's Sunday Magazine and was rather cynical towards these crypto-advocates, nonetheless summarized the situation rather adequately when he wrote:

> The instinctive reaction of most CFP delegates would be to protect software with cryptography, and leave the law out of it...These delegates had no sympathy for governments. This goes right back to their roots, for there is a direct line of descent from the first, libertarian, hippies to the besuited, pigtailed crowd in the Airport Marriott hotel. That descent can be studied by anyone with a computer, a modem, and an account on the WELL, the computer network that set the

[19] Bruce Sterling, "CFP Conference, Topic 92, Comment 77," The WELL, October 1, 1993, well.com)

[20] Efrem Lipkin, "CFP'94 - DATA ENCRYPTION: WHO HOLDS THE KEYS? (Panel)," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 24, 1994), http://cpsr.org/prevsite/conferences/cfp94/encpanel.html/); See also: David Gans, "CFP Conference, Topic 98, Comment 99," The WELL, April 18, 1994, well.com)

> freewheeling tone for the Internet…Its first manager, Cliff Figallo, had lived for 17 years on the Farm, one of the first and most successful of the communes to spread out of Haight-Ashbury.[21]

But, the NSA and other governmental entities didn't go down without a fight. The Cold War infrastructure that spawned the NSA was deeply wary of open systems and relinquishing control in an era so heavily dominated by national security concerns.

The State Fears Open Systems

In the 1990s, the NSA found itself at a crossroads. It chose to reevaluate the enemy and replace the USSR with a conglomerate of social miscreants that included pedophiles, drug dealers, rapists, terrorists, and hackers. The NSA retrofitted their wartime armature into law enforcement and governmental security infrastructure.

As an Apple, Inc., librarian asked in 1992, "with a lot of federal agencies really searching around how to mold swords into plowshares, what do you think the NSA will be doing maybe in the next year?"[22] His question is quite telling because it not only encapsulates the transformation happening at the NSA, but also reflects its reluctance to partake in open and public dialogue. The NSA was transforming their Cold War "swords" into something entirely different. "Plowshares" in this case was a governmental security support and law enforcement support agency.

The National Security Agency was founded in November of 1952 as it evolved from the signal intelligence of World War II. The NSA charter explicitly stated that the agency shall not produce finished intelligence reports. As a juggernaut of intelligence reporting, however, it had massive influential power. Its primary consumers were the "White House, the National Security Council, the Secretary of Defense, the Secretary of State, the Secretary of Treasury, the Secretary of Energy, the Secretary of Commerce, the Federal Bureau of Investigation, the CIA, the Defense Intelligence Agency, the Joint Chiefs of Staff, the three service intelligence agencies, all unified and specialized military commands, military operational commanders (as required), and the intelligence agencies of collaborating foreign nations."[23]

As a producer of signals intelligence (SIGINT), as opposed to human intelligence (HUMINT)—the use of on-the-ground agents and spies—the NSA was able to penetrate the Iron

[21] Andrew Brown, "CFP Conference, Topic 111, Comment 121," The WELL, May 3, 1995, well.com)

[22] Steven Cissler, "CFP'94 - DATA ENCRYPTION: WHO HOLDS THE KEYS? (Panel)," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 24, 1994), http://cpsr.org/prevsite/conferences/cfp94/encpanel.html/)

[23] Matthew M Aid, "The National Security Agency and the Cold War," in Secrets of Signals Intelligence During the Cold War: From Cold War to Globalization (London: Routledge , 2013), 27.

Curtain in ways that more conventional forms of espionage could not. However, in 1989, the Cold War came to an abrupt end with the fall of the Berlin Wall. As a historian of signal intelligence argued, by that time "SIGINT had achieved a preeminent status within the American intelligence community, supplanting (if not actually submerging) the more traditional manpower intensive intelligence sources" that Vice Admiral William O. Studeman considered "historically less productive intelligence means."[24] Interviews with ex-NSA agents revealed an early acceptance, by some, of the inevitability that the "curtain of secrecy would eventually have to come down." In 1946, one of the founding fathers of the NSA, Solomon Kullback even mentioned "[it] is obvious that we cannot hope to keep the cryptologic achievements of the United States and Great Britain completely secret for an indefinite or large number of years."[25]

The contestation between crypto-advocates and the NSA was nothing new. Admiral Bobby Ray Inman who was the NSA director from 1977 to 1981 and acting chair of the President's Intelligence Advisory Board from 1991 to 1993 in many ways embodied the Cold War "dinosaurs" crypto-advocates denounced. He was the NSA poster child of intelligence agency totalitarianism which they despised. Shortly after Inman took office at the NSA in late 1977, Inmahn approached George Davida and several University of California academics in an attempt to stall their push for public encryption. An NSA document described the encounter as "[Inman] found himself in a room with antiestablishment faculty members, and 'for an hour it was a dialogue of the deaf.'" It was only when the vice chancellor of the University of California, Michael Heyman, spoke up and supposed "if 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."[26]

Those at the NSA who espoused Inhman's approach viewed national security as a concern which took precedence over any and all technological advancement in the public realm. With that said, however, many NSA staffers also considered that position as untenable in the post-Cold War period. One NSA document detailed: "[For national security] it was essential, then, to slow the rate of academic understanding of these techniques in order for the NSA to stay ahead of the game. (There was general recognition that academia could not be stopped, only slowed.)"[27]

[24] Ibid, 28.

[25] Ibid.

[26] Thomas R Johnson, "American Cryptography during the Cold War, 1945-1989," 3 American Cryptography during the Cold War, 1945-1989 § (1998), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf), 237.

[27] Ibid, 236.

National security arguments only got the NSA and FBI so far. Even within the NSA, there was a certain fear that having fought monsters for so long, they might be becoming the very thing they had fought against. Recently declassified NSA documents make it clear that there was an internal push for more openness in the post-Cold War era.

The documents that have been declassified by the NSA illustrate that this would be no easy task. Although many in the NSA readily accepted the end of the Cold War curtain of secrecy, the documents tell a story of fear over the inevitable change occuring, a clamoring for meaning, and a switch from an aggressive offense over cryptologic methods to one of reactionary defense in the years following the fall of the Soviet Union. When William Oliver Studeman resigned as NSA director in 1992, he wrote to the entire agency in a memorandum that told of the new world emerging before the eyes of the American people and the agency. "[The] NSA will be increasingly visible to the world, and this openness needs to be thoughtfully, yet fearlessly, managed." He felt as if "the NSA [was] up to this great challenge by aggressively adapting to the new world, both as individuals and as a global enterprise."[28] Studeman seemed to have witnessed reluctance and fear of change occurring at the NSA in the early 1990s. He was most likely advising the incumbent, John M. McConnel, and the higher ups of the need for radical restructuring. Based on the declassified documents on the NSA digital archive and more specifically articles from Cryptographic Quarterly, this shift would not happen without a fight.

One such NSA Cryptographic Quarterly article made the case that the NSA's reluctance to release its grasp on public encryption was rooted in "a reluctance on the part of dinosaurs of the cold war to protect our appropriations."[29] The NSA Director Studeman reiterated fears of budget cuts in his resignation memo, stating, "budget cuts and NSA's relative piece of the intelligence resource pie will likely diminish" in the years after 1992.

NSA officials also feared the economic impact of maintaining such strict control over encryption technology. For instance, in a Cryptographic Quarterly article discussing the viability of supercomputers in the 1990s, when personal computers, PCs, were becoming more and more common, they came to the conclusion that export control over cryptography was costing them much more than they initially realized. The cost of purchasing supercomputers from vendors was skyrocketing in part because of the restrictions on exporting such hardware, which contained encryption methods. They concluded that liberalizing the American marketplace, through looser export controls, was essential for continued operations of their organization.[30]

[28] W. O. Studeman to All National Security Agency Employees, April 8, 1992, NSA DOCID: 3959496.

[29] Cryptographic Quaterly, Winter 1992, Vol. 11, No. 4, "Facing the Post-Cold War Era", NSA DOCID: 3928966

[30] "NSA and the Supercomputer Industry," Cryptographic Quarterly 14, no. 4 (1995), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/NSA_and_the_Supercomputer.pdf)

The NSA slowly began to acknowledge that open-systems were the way of the future. The reality prophesied by NSA personnel such as Kullback was rapidly coming to fruition. If the NSA continued to maintain the same level of closed information, it would render them antiquated.

> The New World Informational Order: A combination of changed geopolitical circumstances and more effective information technology has altered the balance between open-source and restricted information. In both availability and value, the balance has shifted in the direction of—through not fully in favor of—open source information. Moreover, this process is likely to continue, effectively devaluing efforts at informational restriction...In the new informational order, we will be forced to pay far more attention to efficiency, not only because we will have fewer resources to waste but because our overseers will be far more critical in assessing the costs versus benefits of open versus classified information.

However, engaging in a more open environment would be no easy task for the NSA, which was built from the ground up with restricted information in mind. An entire article in the Winter 1989 issue of Cryptographic Quarterly debated the liberal and conservative viewpoints of bringing third party nations into the folds of encryption methods. NSA conservatives retained a Cold War distrust and feared that any sort of assistance in the realm of cryptography towards American allies would reduce the advantage the NSA had over those nations.[31]

NSA liberals understood the changes which were taking place and that these more antiquated policies would not function in the coming years. These arguments surmised that the NSA was "obliged to come out of the closet and deal much more openly with them about cryptologic matters."[32] They could no longer "plan on retreating into some cryptologic Fortress America...The era of U.S. military/economic world dominance is over. We must learn to deal with friendly nations on a more equal basis."[33]

However, the NSA continued to deliberate on its primacy in the declining Cold War environment. "In times of crisis [such as the Cold War and acts of terrorism], societies move to defend themselves by methods that would be neither required nor tolerated in more tranquil environments." The war, which proved a rough master in the Cold War, was no longer a reality in the early 1990s, so a different kind of enemy was needed for NSA relevancy. In searching for

[31] "Third Party Nations: Partners and Targets,," Cryptographic Quarterly 7, no. 4 (1989), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/third_part_nations.pdf)

[32] Ibid.

[33] Ibid.

that which society would not tolerate in the early years of the 1990s, the NSA focused on terrorists, drug dealers, child rapists, and murderers as public enemy number one.[34] The NSA built their plowshares on the basis of protecting society from these new threats. They made claims at the CFP conferences that only "bad guys" were the ones who needed military-grade encryption standards.

In 1993, the FBI made several arrests of suspected cyberterrorists at CFP'94. For instance, a young computer science student from Columbia University, Lee Nussbaum, was arrested at 8:00 in the morning on Friday March 25, 1994. He was suspected to be a notorious hacker by the name of Kevin Mitnick.[35] Bruce Koball spoke to a number of individuals from the core hacker demographic of the CFP conference and noted that none of them were discouraged from attending future conferences, even though they were concerned about the flurry of arrests. Jim Settle of the FBI even went so far as to address the concerns of the community in a special gathering that very evening. Sadly the proceedings of that session are no longer available; however, it seems that he more or less was able to calm the nerves of the group.[36] Although each of the arrests proved to be preemptive moves on mistaken identities, a more active and invasive crackdown by federal agents was perhaps influenced by the events which transpired only months before the conference. These included the bombing of the World Trade Center on February 26th and the infamous Waco compound siege by the ATF and the FBI that lasted from February 28th through April 19th of 1993.

The NSA Opens Up

Open access to information—catalyzed by new emerging technologies such as the internet—was the coup de grâce for the Cold War closed information culture in the United States. Cryptographic Quarterly encapsulated this trend in an article titled "Facing the Post Cold War Era". It asserted that the:

> The end of the cold war is the most dramatic of the fundamental changes that will affect NSA's future, but a radical transformation of information technology may be even more basic in its impact and contributed significantly to the collapse of

[34] Ibid; Stuart Baker, "CFP'94 - DATA ENCRYPTION: WHO HOLDS THE KEYS? (Panel)," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 24, 1994), http://cpsr.org/prevsite/conferences/cfp94/encpanel.html/)

[35] Bruce Koball, "CFP Conference, Topic 98, Comment 18," The WELL, March 25, 1994, well.com)

[36] Ibid.

> the Soviet Union. Finally, the American political climate towards intelligence has changed, largely because of changes in the threat and information environments.[37]

In a surprising turn of events, NSA leadership listened to their own more liberal staffers viewpoints on openness. Perhaps influenced by Democrat Bill Clinton taking executive office in 1993, there was an unprecedented appearance of the NSA at the CFP Conferences. At CFP'94, Stuart Baker, the general counsel of the NSA, spoke to the crypto-advocates directly and attempted to convey the official NSA perspective to the crowd. Bruce Koball vocalized this surprising turn of events at CFP'94. Even though "the NSA's foray into public discussion [was] heavily seasoned with arrogance and even contempt for the reasoned arguments of the opposition," the very fact that they showed up and openly talked to this group of crypto-advocates sent the bigger message. The NSA was coming out of the closet. Their public presence was "a tacit admission that this issue will not submit to their usual approach ('trust us..we know what's best for national security…')."[38]

Baker spoke mainly of his concern about the "sanctuary" technologies like encryption would create for criminals such as terrorists, drug dealers, child rapists, and murderers. He emphasized that society couldn't "know what it is going to be like if criminals or terrorists or other people who are hostile to society can use that sanctuary to communicate." He surmised that "it probably [would not] be as pleasant in terms of freedom from crime and terror as the world we live in today." As Baker saw it, Clipper was something to help protect society from the edge given to bad guys by emerging technologies.[39]

When others rebuked Baker and gave PGP as an example of non-governmental encryption which functioned superbly without government intervention, Baker retorted by again emphasizing the need of government protection from pedophiles.

> PGP, you know, [is believed to be] out there to protect freedom fighters in Latvia or something. But the fact is, the only use that has come to the attention of law enforcement agencies is a guy who was using PGP so the police could not tell what little boys he had seduced over the net. Now that's what people will use this for—not the only thing people will use it for but they will use it for that and by insisting on having a claim to privacy that is beyond social regulation we are creating a world in which people like that will flourish and be able to do more

[37] Cryptographic Quaterly, Winter 1992, Vol. 11, No. 4, "Facing the Post-Cold War Era", NSA DOCID: 3928966

[38] Bruce Koball, "CFP Conference, Topic 98, Comment 112," The WELL, April 26, 1994, well.com)

[39] Stuart Baker, "CFP'94 - DATA ENCRYPTION: WHO HOLDS THE KEYS? (Panel)," CFP'94 - Index (CPSR: Computer Professionals for Social Responsibility, March 24, 1994), http://cpsr.org/prevsite/conferences/cfp94/encpanel.html/)

> than they can do today...
>
> we have some responsibility for that and therefore we have some responsibility to design and use encryption that (if it does migrate to the private sector) does not put law enforcement out of business.

Such paternalist notions in regard to protecting the people from threats were common among the law enforcement and especially the intelligence agency communities at the CFP conferences. Emerging from the Cold War climate, these fears were not an abstract grasping for relevancy, but rather a reality. Even in the pre-9/11 world, by the mid 1990s, terrorism was becoming a common fear as evidenced by the World Trade Center bombing and the federal seige at Waco. These individuals, such as Stuart Baker and Don Ingraham (Assistant District Attorney of Alameda County, California), played upon these fears to further their beliefs on the emerging cyberculture.

However, actions speak louder than words. NSA used to be an agency which was so secretive that its existence was redacted from government communications. The agency whose existence was once denied by the government was now openly sending delegations to public conferences and representing their viewpoint, on the defense no less. The significance of this development cannot be understated. The days of sending cease-and-desist letters threatening jail time to academics such as George Davida had passed. These Cold War tactics of governmental threats veiled in the name of national security were dwindling. Perhaps John Gilmore of the EEF said it best in 1992:

> It's clear that there was no reason to doubt what the NSA said over the last 40 or 50 years, because there was no harm if you followed their regulations. Maybe 10 people got hurt, or 20 people got hurt that year, and you could afford that for national security. *But when the privacy of millions of people who have cellular telephones and the integrity of our computer networks and our PCs against viruses are up for grabs here, then I think the battleground is going to be counting up the harm and in the public policy debate trying to strike a balance. The real challenge there will be to get the people who can show harm on the other side, who can show harm to our national security by freeing the technology, to speak up and tell us what this harm is. They're so unused to having to defend the need for it that I'm afraid they will just sort of attempt to push it to the wire, and whether they win or lose is not the issue. The result will be not what's best for the country.*[Accentuation is mine][40]

[40] John Gilmore, "CFP'92 - Who Holds the Keys?," CFP'92 - Index of Papers (CPSR: Computer Professionals for Social Responsibility, March 20, 1992), http://cpsr.org/prevsite/conferences/cfp92/denning.html/)

CFP participants rejected Baker's arguments wholesale as the crypto-advocates rallied in unison. WELL user and CIA analyst, Ross Alan Stapelton-Gray, who went by the username "Amicus," was one of the most prominent antagonists to the national security concerns of the NSA and FBI. He said it best when he argued that "other problems of increasing information accessibility [encryption], such as 'stalking' or other crimes, will have to be dealt with as a crime problem, and not a 'criminals access to more information' problem."[41] Issues such as stalking, rape, pederasty, murder, terrorism, and drug dealing were problems of crime and shouldn't be seen as an issue inherent in technology.

Bruce Sterling considered the position espoused by the NSA and the FBI to be absurd. He referenced pedophilia, child pornography, and deviant sexual behavior as "specious blackwash" by the NSA and FBI. He saw this as a political maneuver that aimed to paint those who wanted public encryption as criminals who would delegitimize their claims. He asked if Americans are "so neuroitically uptight about deviant sexual behavior that we will allow our entire informational structure to be dictated by the existence of pedophiles?"[42] His point here was not to defend pedophila, but rather to highlight the intelligence community using strawman arguments and scapegoats to further their own political ends. Sterling concluded that the "Four Horsemen of Kidporn, Dope Dealers, Mafia, and Terrorists"[43] are nothing when compared to the issues of a totalitarian government.

Although transcripts of later conferences are lost, it is clear that by 1996, the NSA regularly sent delegations to the CFP conferences. While the NSA integrated itself in the public dialogue over opening up encryption methods, they were not alone. A piece of the puzzle that generated much debate amongst crypto-advocates was the role of private industry. While they were skeptical of large bureaucracies and organizations, having an ally with as much sway as corporations such as Microsoft would prove effective. As corporations began to send delegations to the CFP, they also brought mainstream interests to the Net. Once America began to come online, the crypto-advocates realized the double edged sword was swiftly cutting them out of the equation.

Private Industry Moves In: America Comes On-Line

The sense of urgency these crypto-advocates felt for opening up encryption methods was partly a manifestation of their sense as pioneers on the electronic frontier. They quickly began to

[41] Ross Alan Stapleton-Gray, "CFP Conference, Topic 98, Comment 137," The WELL, May 2, 1994, well.com)

[42] Bruce Sterling, "CFP'94 - Bruce Sterling on Privacy," CFP'94 - Index of Papers (CPSR: Computer Professionals for Social Responsibility, March 26, 1994), http://cpsr.org/prevsite/conferences/cfp94/sterling.html/)

[43] Ibid.

realize, however, that they were not alone. Industry and the new informational economy that coalesced after the Cold War were quickly gaining traction. During the first CFP Conference, these crypto-advocates invited a large number of academics, lawyers, and law enforcement. After CFP 1, however, they quickly realized they had made a huge mistake by not inviting people from the private sector. As they realized the private sector, such as banks and computer manufacturers, needed access to better public encryption, they invited them to participate too.[44]

The only industry firm that participated in CFP'91 was Equifax. They attempted to establish a linkage of trust with the crypto-advocates. David Mooney of Equifax articulated "as our corporate name implies, Equifax realizes and accepts that we have a responsibility for equity and fairness in the handling of factual data...we acknowledge this position of trust."[45] After CFP'91, Bruce Koball and other crypto-advocates on the WELL debated the future of the conference and which demographics needed to be included. Including industry beyond just Equifax was one of their top priorities.[46]

Although they were able to bring together "law enforcement (LE) representatives from state, local, and federal governments, civil libertarians, and convicted computer criminals, as well as some victims"[47] of cybercrime, they needed to do something about bringing larger constituencies into the fold. CFP'92 was subsequently held at the seat of federal power in Washington, DC and they made a concerted effort going forward to fill the conference with speakers from industry—Apple, Citicorp, AT&T, Equifax, IBM, etc.

At CFP 1993, as the FBI was making inquiries and arrests, these crypto-advocates turned toward industry for support as capstoned by Dorthy Denning's (Georgetown University) speech on the positives of industry offsetting government overreach. Her presentation, which was titled *To Tap or Not to Tap* and focused on the ethics of wiretapping, also acted as a call to unite the crypto-advocates behind the forces of industry. She argued that "because the only people who would have access to the systems for activating a tap would be employees of the service providers, who have been strict about requiring court orders, the possibility of law enforcement performing unauthorized taps seems even less likely than with present technology."[48] In a sense, she was arguing that industry could be trusted to protect its interests in the consumer. Industry

[44] Bruce Koball, "CFP Conference, Topic 60, Comment 11," The WELL, July 2, 1991, well.com)

[45] David J Mooney, "Social Responsibility in the Information Age," CFP'91 - Index (CPSR: Computer Professionals for Social Responsibility, 1991), http://cpsr.org/prevsite/conferences/cfp91/equifax.html/)

[46] Bruce Koball, "CFP Conference, Topic 60, Comment 11," The WELL, July 2, 1991, well.com)

[47] Steven Cissler, "CFP Conference, Topic 72, Comment 11," The WELL, April 9, 1992, well.com)

[48] Dorthy E Denning, "CFP'93 - To Tap or Not to Tap," CFP'93 - Index of Papers (CPSR: Computer Professionals for Social Responsibility, March 1993), http://cpsr.org/prevsite/conferences/cfp93/denning.html/)

could act as an intermediary between the interests of law enforcement and the interests of the consumer, or in this case the crypto-advocates.

Perhaps Andrew Brown said it best when he reported that “it is not just terrorists, libertarians, and the citizens of totalitarian countries who need strong encryption.” Rather, “large companies which shuffle huge quantities of financially sensitive information around the world” require these measures to provide essential commerce and services on the emerging platforms. The only way they could do this safely was through encryption. “The strongest lobbying against US arms control regulations in this area comes from companies like Microsoft, which want to build strong encryption into their business products and export them around the world.”[49]

Lance Hoffman of George Washington University argued that “With the end of the Cold War, some foriegn nations may turn their espionage apparatus into a tool for industrial espionage, making U.S. companies targets of intelligence-grade threats seeking industrial secrets.”[50] If the U.S. government mandated trap doors in encryption, it would leave American companies vulnerable to such spying. The interests of industry and the interests of crypto-advocates, at least from Hoffman and Dennings viewpoints, were much more aligned and intertwined.

1993 and 1994 were large turning points in power dynamics at the CFP conferences. FBI agents knocked on hotel rooms at CFP’93 claiming to be “room service” and interrogated participants' at the same time as Dennings and Hoffman argued that industry can be trusted and was essential for furthering their desire to make encryption public. Even though the contacts crypto-advocates were forging at the conference were proving beneficial, the shift towards industry was significant.

Jim Settle, an FBI agent who was a regular contributor at the CFP conferences, “was sincerely concerned about the incidents that occured, to such an extent that he held an informal BOF (birds-of-a-feather) session after the last session of the [conference] on Saturday and answered questions from a crowd of about 100 sometimes-hostile folks in as frank and open a manner as he felt able to do.” Bruce Koball concluded “this young and sometimes-fractious community will be seriously tested, but I believe that even such institutions as the nation’s ‘premier spookocracy’ can be turned. Institutions are ultimately individuals and individuals can talk to each other.”[51] Seeing the contacts they were forging ultimately as individuals ultimately helped the crypto-advocates accept the help of larger bureaucracies such as in industry and law enforcement.

[49] Andrew Brown, “CFP Conference, Topic 111, Comment 121,” The WELL, May 3, 1995, well.com)

[50] Lance J Hoffman, “CFP'93 - Will ‘Usually Secure’ Cryptography Permit Bugging of the Digital Network?,” CFP'93 - Index of Papers (CPSR: Computer Professionals for Social Responsibility, 1993), http://cpsr.org/prevsite/conferences/cfp93/hoffman.html/)

[51] Bruce Koball, “CFP Conference, Topic 98, Comment 18,” The WELL, March 25, 1994, well.com)

After 1994, it was clear that the power dynamics at the CFP conference had shifted. As industry became a larger player in the debate over public encryption, so too was there more news coverage of the conference as well as a more mainstream debate over these emerging Internet technologies. Radio, cable, and newspaper coverage of the debates as well as a general familiarity of the Internet began to skyrocket after 1993.[52] Robert Steele, another CIA WELL user made the claim at CFP'94 that the Computer, Freedom, and Privacy conference was ready for the big time now that it was garnering lots of media attention.[53] Another WELL user, Kathy Watkins, remarked on her experience speaking at CFP'95 that she "was pretty surprised to find tv cameras there," but that such coverage had become commonplace.[54]

As more Americans became familiar with the Internet and the culture gap closed, crypto-advocates suddenly realized that they no longer had the same agency they once had. In 1995, Mike Godwin of the Electronic Frontier Foundation mentioned that "some of the polarization comes from the fact that what were fringe issues in 1991 are now mainstream policy issues—so the debate *matters* more." Andrew Brown rather continued with the issue:

> Now, arcane techniques like public key encryption which were until recently the province of obscure mathematicians and hobbyists are becoming essential to the security of big money and international trade on computer networks. And the networks themselves, once the happy playground for the smartest kids in the world, are now providing a reliable global communication system for the sort of people who believe that freedom of speech, the Internets glory, is open to abuse and needs to be controlled…
>
> None of this would matter if the Internet were still a private world for clever students. But after years of saying that it is going to take over the world, the Internets champions have been horrified to discover that this is true; and the takeover is mutual.[55]

Crypto-advocates, such as Ross Stapelton-Gray, slowly realized that the time of pioneers on the electronic frontier had passed. They were no longer a small vanguard of expert Net dwellers, but rather members of a growing metropolis. This metropolis extended citizenship to thousands of new users across a multitude of society's sectors. Gail Williams remarked in 1995, "in some ways, what we do now as individuals in this environment doesn't feel like pioneer days

[52] See well.com, CFP Conference, Topic 96

[53] Robert Steele (CIA), "CFP Conference, Topic 98, Comment 82," The WELL, April 3, 1994, well.com)

[54] Kathy Watkins, "CFP Conference, Topic 111, Comment 25," The WELL, March 31, 1995, well.com)

[55] Andrew Brown, "CFP Conference, Topic 111, Comment 121," The WELL, May 3, 1995, well.com)

so much. It turns out that law extends into space. Or on to the prairie. The questions are mostly how, not if."[56] Ross Stapelton-Gray remarked that perhaps the time of Net pioneers had given way to Net town-builders of which they were no longer the main demographic.[57]

The sense of fleeting urgency, diminishing influence, and shifting power dynamics was palpable in a remark made by WELL user John Seabrook after CFP 1995.

> At last year's cfp the Clipper Chip was a monster that gave urgency and moral beauty to the proceedings, it really felt like everyone was pulling together to preserve our liberty. This year, with the Clipper battle basically won...it felt like much had changed. The utopian feeling was still there, but it seemed tired; it had a routine quality. For the first time I had the feeling, again depressing, that the red hot center of net thought might be elsewhere, perhaps at a conference devoted to net commerce, not net liberty.[58]

University of Pennsylvania Professor Matt Blaze cracked the Clipper Chip encryption in 1994 and illustrated how "you can't build a door into strong encryption and only expect the good guys to ever figure out what the key is, to ever have a key to it. If you're going to weaken the encryption, they'll let the good guys have a key. You're going to weaken the encryption such so that the bad guys will have access too."[59] Cindy Cohn, Executive Director of the EFF continued that this essentially the coup de grâce whereby crypto-advocates triumphed over governmental regulation. The governmentally-endorsed DES algorithm, with its 56-bit key length requirement, was also cracked by cryptographers by 1997 so that any message encrypted by DES could be read in just under 22 hours. With the Clipper Chip and DES dead in the water, the government gave into the demands of crypto-advocates and industry.[60]

Conclusion

Stemming from the counterculturalist movement of the 1960s, crypto-advocates rallied together on emerging technologies. In doing so, they created a sense of identity as pioneers on the electronic frontier of which they were the prime constituency. After the fall of the Soviet Union and the adoption of personal computers, these crypto-advocates understood the

[56] Gail Williams, "CFP Conference, Topic 111, Comment 46," The WELL, April 4, 1995, well.com)

[57] Ross Alan Stapleton-Gray, "CFP Conference, Topic 111, Comment 48," The WELL, April 4, 1995, well.com)

[58] John Seabrook, "CFP Conference, Topic 111, Comment 42," The WELL, April 3, 1995, well.com)

[59] Darknet Diaries, *Crypto Wars*, February 1, 2018, https://darknetdiaries.com/transcript/12/); Interview with Cindy Cohn.

[60] Ibid.

possibilities that existed for communicating over the Internet. They also understood the need for ensuring privacy and accountability on the new platforms. From 1991 to 1996, they gathered at such places as the Computer, Freedom, and Privacy conferences and on the WELL to discuss their ideas and their strategies for change. At CFP, they made lasting connections with individuals from a wide array of backgrounds such as academics, non-profit activists, computer scientists, librarians, and most importantly, law enforcement and intelligence agency personnel. They confronted those individuals and agencies they saw as agents of an increasingly totalitarian enterprise during the Cold War. Although they sparked the movement for public encryption, something which we enjoy today, their voices were drowned by the great swell of industry interests in the emerging post-Cold War informational economy.

By 1996, radical changes were taking place at the federal level related to the government's approach to cryptography. The watershed moment was the passage of Executive Order 13026, which was signed into effect by Bill Clinton on November 15, 1996. This executive order moved "export controls of encryption products" regulated by the United State Munitions List to the Commerce Control List. Essentially, this meant that governmental encryption regulation was moved from the State Department to the Commerce Department—from military/intelligence agency control to civilian control. No longer was encryption considered an aspect of military operations alone, but rather, it became an integral part of the post-Cold War society. By the close of the decade, the U.S. government officially dropped all court cases challenging academics' use of cryptography. In addition, they also stopped requiring licensing and restricting key lengths, such as under DES, altogether.[61]

Even though by the close of the decade, the first Crypto War had come to an end, the battle for encryption privacy is ongoing. Today the news is riddled with stories arguing for or against privacy from government and corporate intrusion. For instance, in March 2020, amidst the COVID-19 pandemic, Congress debated a bill called the EARN IT Act. This bill sought to limit encryption technology. The crux of the matter, related to child pornography, registered with cryptography experts. Heather West of Mozilla said "The EARN IT Act would cause great harm to the open Internet and put everyday Americans at greater risk — creating problems rather than offering a solution."[62] Many of the same issues fought today stem from the same issues brought up and encountered by crypto-advocates after the fall of the Berlin Wall. Although the crypto-advocates were successful in democratizing encryption, the debate over a society undergirded by either personal privacy or national security is far from over.

[61] Darknet Diaries, *Crypto Wars*, February 1, 2018, https://darknetdiaries.com/transcript/12/); Interview with Cindy Cohn

[62] Joseph Marks, "The Cybersecurity 202: Cybersecurity Experts Slam Child Protection Bill That Risks Rolling Back Encryption," *The Washington Post*, March 30, 2020, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/03/30/the-cybersecurity-202-cybersecurity-experts-slam-child-protection-bill-that-risks-rolling-back-encryption/5e80cfd5602ff10d49ad761a/)

Bibliography

Aid, Matthew M. “The National Security Agency and the Cold War.” In Secrets of Signals Intelligence During the Cold War: From Cold War to Globalization, 27–64. London: Routledge , 2013.

The Computers, Freedom, and Privacy Conference. CFP.org, n.d. http://www.cfp.org/.

“CPSR Conferences and Events.” Computer Professionals for Social Responsibility. CPSR, n.d. http://cpsr.org/prevsite/conferences/index.html/.

“Declassification and Transparency Index.” Declassification and Transparency. National Security Agency, n.d. https://www.nsa.gov/news-features/declassified-documents/.

Edwards, Paul N. Closed World: Computers and the Politics of Discourse in Cold War America (Inside Technology). MIT Press, 1996.

Hellegren, Z. Isadora. “A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom.” Internet Histories: Digital Technology, Culture, and Society 1, no. 4 (October 23, 2017): 285–311. https://doi.org/10.1080/24701475.2017.1387466.

Igo, Sarah E. Known Citizen: A History of Privacy in Modern America. Harvard University Press, 2018.

Levy, Steven. Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age. New York, NY: Penguin Books, 2001.

Rider, Karina. “The Privacy Paradox: How Market Privacy Facilitates Government Surveillance.” Information, Communication & Society 21, no. 10 (October 3, 2018): 1369–1385. http://www.tandfonline.com/doi/abs/10.1080/1369118X.2017.1314531.

Turner, Fred. “Where the Counterculture Met the New Economy.” Technology and Culture 46, no. 3 (July 2005): 485–512.

Turner, Fred. From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. Chicago: The University of Chicago Press, 2008.

WELL.com. The Whole Earth Network, 1985-2020. https://www.well.com/.