# U.S. Export Controls on Encryption Technology

by

Shirley K. Hung

A.B. Government
Harvard College, 2000

SUBMITTED TO THE DEPARTMENT OF POLITICAL SCIENCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN POLITICAL SCIENCE
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

SEPTEMBER 2004

Signature of Author: ______________________________
Department of Political Science
August 20, 2004

Certified by: ______________________________
Kenneth A. Oye
Associate Professor of Political Science

Accepted by: ______________________________
Stephen D. Ansolabehere
Professor of Political Science
Chair, Graduate Program Committee

# U.S. Export Controls on Encryption Technology

by

Shirley K. Hung

Submitted to the Department of Political Science
on August 23, 2004 in Partial Fulfillment of the
Requirement for the Degree of Master of Science
in Political Science

## ABSTRACT

This thesis seeks to explain why the U.S. government export controls on encryption technologies instituted during the 1970s remained in place until 1999 even though the widespread availability of similar products internationally had rendered the regulations largely without national security benefit by the late 1980s and early 1990s. The second part of the thesis explores the processes and reasons behind the eventual liberalization of encryption policies in 1999. Underlying the study is a values tradeoff between national security, economic interests, and civil liberties for which the relative gains and losses to each value shift through the three decades of the study as a result of technological advances in commercial and civilian cryptography, the growing popularity of electronic communications, the rise of the computer software industry, and the end of the Cold War.

The explanation rests upon a combination of political science and organization theories. Structural obstacles to adaptation within the legislative process and interest group politics help account for some of the inertia in the policy adaptation process. In particular, regulatory capture of the Presidency and critical Congressional committees by the National Security Agency helped lock in the NSA's preferred policies even after technological advancements in the commercial sector began to cut into the national security benefits resulting from export controls. Interest group politics also helps explain the rise and eventual success of the lobby for liberalization of encryption regulations. A combination of the software industry and civil liberties activists intent on preserving the right to privacy and First Amendment allied to lobby Congress to change encryption regulations, an effort that eventually paid off in 1999. Interest group politics also factors into the actions of the national security establishment as they also lobby the Presidency and Congress to maintain restrictive encryption regulations. The study uses organizational culture to explain the motivations and some of the actions of the NSA, particularly with regard to its preference for secrecy, its placement of national security above other values, and its efforts to maintain control over all cryptology, whether government or civilian.

Thesis Supervisor: Kenneth A. Oye

Title: Associate Professor of Political Science

## Acknowledgements

In writing these acknowledgements, I begin to realize how little of this thesis truly belongs to me. The number of people who have supported me financially, intellectually, and personally during the past few years is too numerous to list, so I hope those who I have left off will forgive me.

I would like to thank the supporters of my research, the National Science Foundation, the MIT Department of Political Science, and the MIT Center for International Studies/ Security Studies Program.

I would also like to thank the members of the MIT faculty and staff who have guided me through my time in graduate school. To Monica Wolf, who has moved to sunnier climes, and Susan Twarog, many thanks for unfailing competence and cheerfulness – and perspective – in the face of the graduate student blues.

I would especially like to thank my advisor Ken Oye for not only supervising my thesis, but for sparking so many of the ideas in it and providing both intellectual and moral support before and during its writing. To find someone whose intellectual interests are as broad as his energy and kindness to his students is a rare thing indeed.

I owe a special debt of gratitude to Steve Rosen of Harvard University, who went above and beyond the call of duty to serve as a reader on this thesis despite having already suffered through my undergraduate thesis. I frequently wonder at his tolerance for having put up with me since I was a teenager and all the awkward years since – and more that he is still willing to speak to me despite it! I only wish I had the words to express how much his guidance, his caring and his friendship has meant to me.

To my friends, who during the past months I have dragooned into serving as sounding boards, editors, proofreaders, human thesauri, personal assistants, food delivery services, and physics/ computer science teachers, many thanks are due. Chung, Jake, and especially Loretta – this thesis would not exist without you. Whether that is a good thing or not is another story.

The final thanks go to my family, which never once asked what I was writing about and kept things in perspective by constantly reminding me that no one would actually read this thesis. I promise, I will finish soon and get a real job.

## Table of Contents

## List of Abbreviations

| | |
|---|---|
| AFSA | Armed Forces Security Agency |
| CBO | Congressional Budget Office |
| CCEP | Commercial Communications Security Endorsement Program |
| CIA | Central Intelligence Agency |
| CoCom | Coordinating Committee for Multilateral Export Controls |
| COMINT | Communications Intelligence (see SIGINT) |
| COMSEC | Communications Security (see IA) |
| CSA | Computer Security Act (1987) |
| DCI | Director of Central Intelligence |
| DES | Digital Encryption Standard |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| EC | European Commission |
| EES | Escrowed Encryption Standard (Clipper Chip) |
| EFF | Electronic Frontier Foundation |
| EPIC | Electronic Privacy Information Center |
| FBI | Federal Bureau of Investigation |
| FOIA | Freedom of Information Act |
| GAO | Government Affairs Office |
| IA | Information Assurance (see COMSEC) |
| IEEE | Institute of Electrical and Electronics Engineers |
| ITAR | International Trade in Arms Regulations |
| JCS | Joint Chiefs of Staff |
| MOU | Memorandum of Understanding |
| NBS | National Bureau of Standards |
| NIST | National Institute of Standards and Technology |
| NRC | National Research Council |
| NSA | National Security Agency |
| NSC | National Security Council |
| NSDD | National Security Decision Directive |
| OCR | Optical Character Recognition |
| OECD | Organization for Economic Cooperation and Development |
| OTA | Office of Technology Assessment |
| PGP | Pretty Good Privacy |
| RNG | Random Number Generator |
| RSA | Rivest, Shamir, Adleman – refers both to the RSA algorithm and the company, RSA Data Security (now called RSA Security since its purchase by Network Associates) |
| SIGINT | Signals Intelligence (see COMINT) |
| TWG | Technical Working Group (NSA-NIST) |
| USAID | United States Agency for International Development |
| USCIB | United States Central Intelligence Board |

# Chapter 1

## *The Question*

Failure to adapt to changing external conditions, whether at all or in a timely manner, is a recurring theme in the history of government, bureaucracies, businesses and other large organizations. Failure to adjust policies even in the face of new developments that render the policies ineffective or outdated is one form of this organizational inertia. Frequently, it results from a failure to realize that the outside environment has changed, an inability or unwillingness to adapt, or some combination of the three factors. In this paper I examine national encryption policy from the period 1973-1999, a period during which technological developments in the civilian sector slowly eroded the effectiveness of government export controls established during the early Cold War.

The fundamental debate over national encryption policy centers on the relative weights of three values: national security, economic interests, and civil liberties. Over the course of three decades, changes in encryption technology and the external environment shifted the balance of values at stake in the debate from favoring national security to favoring economics and civil liberties. In the formative period of encryption policy from the 1970s to the late 1980s/ early 1990s, the gains to national security provided by export controls outweighed their impact on the software industry or civil liberties, as the industry was in its infancy and little consumer demand for encryption existed. During the period from the late 1980s/ early 1990s to 1999, however, there was a lag during which national encryption policy was at odds with conditions in the international environment, where strong encryption was readily available from multiple international sources and even downloadable for free off the Internet. In other words, the technology and the policies were out of sync, with little gain to national security and great costs to the software industry and civil liberties imposed by the policies. Only during the period from 1999 to the present did national policy change to rectify this imbalance in the values tradeoff.

The central question of this study, therefore, is why did government policy remain largely unchanged during the period from 1991-1999, despite evidence that it was ineffective? And what prompted the changes in 1999, given the lack of adaptation in the time period before?

I argue that the failure to adapt national encryption policies to the changing environmental conditions even after civilian and international technological developments had rendered government policies ineffective was a the result of a government agency, the National Security Agency, successfully controlling encryption policy in accordance with its own organizational interests and beliefs through regulatory capture and successful conversion of critical components of the government's regulatory structure to its point of view. The subsequent shift in national policy in 1999, which reversed many of the restrictions on export and development of encryption, was brought about by a successful lobbying effort by a combination of the rising computer software industry and civil liberties activists that awakened an interest in encryption policy in previously neutral portions of Congress; a growing awareness of the need for encryption due to the growing popularity of e-commerce and the Internet; and advances in technology that underscored the ineffectiveness of current export policies.

### *The Debate*

#### *The National Security Argument*

The United States relies more upon signals intelligence (SIGINT) than any other type of intelligence.[1] As former Senate Intelligence Committee member Walter Mondale once stated, the NSA is "possibly the most single important source of intelligence for this nation."[2] Since World War II, when the breaking of German and Japanese diplomatic and military codes helped contribute to the Allied victory, shortening the war and saving countless lives, the role of communications intelligence in the American national security establishment has increased dramatically.[3] The communications intelligence community occupies over 80 percent of the nation's intelligence budget and includes a network of satellite dishes, antenna arrays, relay stations and transmitters that span the globe and even outer space, in the air, on the ground, underground and both on and in the ocean. The government agency charged with the greatest responsibility for the collection, processing and dissemination of foreign signals intelligence is the NSA. The NSA, in essence, is a brain with thousands of ears all over the world, which provides intelligence to American military leaders and policy makers "to ensure our national defense and to advance U.S. global interests."[4]

The ability to provide political and military leaders with timely, reliable SIGINT depends upon the ability of the NSA to not only access the information by successfully intercepting foreign communications, but also to sort through, read, and analyze the information contained in those communications. Encryption complicates this task exponentially. First, encrypted communications look like gibberish, making it difficult to identify critical messages. As the volume of encrypted messages goes

[1] I use communications intelligence (COMINT) and signals intelligence (SIGINT) interchangeably in this paper. Both refer to one half of the National Security Agency's mission; the other half is Communications Security (COMSEC), now called Information Assurance (IA).

[2] U.S.S., Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *The National Security Agency and Fourth Amendment Rights,* Hearings, 94th Cong., 1st Sess., p. 35., in James Bamford, *The Puzzle Palace* (Boston: Houghton Mifflin, 1982), 4.

[3] For discussion of ULTRA intelligence (deciphered German, Italian and German diplomatic and military communications, especially the German Enigma-enciphered messages and Japanese Purple-code ciphers) in shortening the war, see Simon Singh, *The Code Book* (New York: Doubleday, 1999), Ch. 4, especially pp. 186-188, and Robert Churchhouse, *Codes and Ciphers: Julius Caesar, the Enigma, and the internet* (Cambridge: Cambridge University Press, 2002). ULTRA is also sometimes referred to as MAGIC, though I have seen MAGIC used more often to refer to communications in the Pacific theatre and ULTRA those in the European theatre.

[4] NSA mission statement. http://www.nsa.gov/sigint/index.cfm

up, the ease of picking out important messages at first glance with a keyword-search like operation goes down. Second, it requires rapid decryption of messages before their contents can be read and analyzed. The decryption process can be slow, arduous, and costly, such that even if successful, it imposes a time lag in obtaining intelligence that may be time-sensitive. These difficulties account for the NSA's objection to diffusion of strong encryption. Although they did not state as such publicly, their true objective was most likely to limit the use of encryption in all electronic and digital communications, or at minimum to limit encryption to weak encryption that could be easily broken in real-time by NSA computers, so as to maintain a high level of plaintext-equivalent communications that could be monitored. Thus, throughout the 1970s-1990s, the NSA and other members of the national security establishment pushed for strong export controls and other restrictions on encryption, arguing that widespread encryption in the hands of unfriendly governments, criminals, terrorists, and other enemies of the U.S. would threaten American national security because it would reduce the speed, quality and quantity of SIGINT.

*The Economic Interest Argument*

The national security establishment was not the only party with an interest in encryption policy. The computer software and financial services industries also had much to gain or lose. As the software industry grew in size and influence, the impact of export controls on their business and their opposition to restrictions on the export and development of encryption grew in proportion. Prior to 1973, cryptography was largely the domain of the NSA. By mid-1973, however, the financial services industry (banks, financial clearinghouses) had begun to adopt electronic communications and processing techniques to manage the huge and growing volume of daily transactions. The computer software industry, in response, developed commercial encryption technologies to service those industries and the industries that would later emerge with a need for secure communications. By the late 1980s and early 1990s, with the booming popularity of e-commerce, electronic communications, and the Internet, the market for encryption had become a global mass market.

During the 1990s, U.S. export controls on strong cryptography were projected to cost U.S. firms anywhere from $50 billion to $97 billion over a five year period,[5] and possibly an additional $140 billion

[5] A study funded by the Computer Systems Policy Project predicted that revenues of U.S. systems suppliers would reach $200 billion by 2000, and that $50 of this could be lost to foreign suppliers as a result of export controls. Reported in William F. Hagerty, *The Growing Need for Cryptography,* 1995, quoted in Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology with Drive Policy," in Brain Kahin and Charles Nesson, *Borders in Cyberspace* (Cambridge, MA: MIT Press, 1997), p. 293. For an alternative estimate of $6 to $9 billion per year, see testimony of Ray Ozzie of Lotus/ Iris Associates, before the House Foreign Affairs Subcommittee on Economic Policy, Trade, and Environment, quoted in John Schwartz, "Bill Would Ease Curbs on Encoding Software Exports," *Washington Post,* November 23, 1993, C1.

in overseas sales.[6] The regulations hampered development of one of the U.S. economy's most innovative and vibrant industries, one that could be considered a strategic or high-value industry, by limiting their sales to less than half their potential market.[7] The software relies upon high sales volume and economies of scale to offset high research and development costs, so the loss of sales disproportionately affects their profit margins. The lower profits, in turn, meant less funding for further R&D and less of a boost to the U.S. economy. In addition, the regulations increased development costs by artificially imposing distinctions between domestic and international versions of the same product, forcing firms to either produce two versions or make a single version with universally weak encryption. The first option saddled firms with the costs of making two systems interoperable, stocking two versions, and the resentment from international customers who were given an inferior product with less security. The latter option instead left all customers with weak encryption, a suboptimal solution for domestic consumers who were allowed stronger encryption. The restrictions also hampered the development of a growing sector of the economy: e-commerce. The anonymous nature of e-commerce required encryption to ensure the security of transactions, from protecting credit card numbers to the identity of the buyer. By hurting the ability of software companies to develop encryption and discouraging use of encryption by consumers, the government also slowed the development of this important sector of the economy.

*The Civil Liberties Argument*

Turning from financial interests to more philosophical concerns, restrictions on encryption threaten basic civil liberties, including the right to privacy, the right to free speech, and even the right against self-incrimination. The right to encrypt communications is fundamentally about the right to privacy, a concept embodied in the UN Universal Declaration of Human Rights.[8] Encryption allows an individual to ensure that his electronic and digital communications and data are not overheard or read by anyone he does not wish to do so, whether by encrypting data on a hard drive, e-mail, or even telephone conversations. The importance of encryption to ensuring individual privacy, corporate information, and even credit card numbers grew exponentially during the period of the study, as digital communications became increasingly integrated into daily life. By restricting access to encryption or imposing restrictions on the types of encryption that could be used, the government in effect curtailed the right to privacy.

[6] I have my doubts about this figure, but the figure comes from Erik R. Olbeter, "Encryption and Security," J. of Com., Aug. 6, 1998, at 7A, cited in cited in F. Lynn McNulty, "Encryption's Importance to Economic and Infrastructure Security," *Duke Journal of Comparative and International Law*, Spring 1999.. I should note that Mr. McNulty is the Director of Government Affairs for RSA Data Security, the country's leading provider of commercial cryptography technology

[7] A typical mass market software company such as Microsoft or Lotus sells more than half of their software overseas.

[8] See Article 12, UN Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." http://www.hrweb.org/legal/udhr.html

Encryption regulations also threatened First Amendment rights to free speech. In the 1990s, federal courts ruled that the source code of encryption programs and text of academic papers discussing algorithms and encryption techniques constituted a form of speech. Federal export controls on publication of encryption software code, as well as the NSA's practice of pre-publication review of academic papers on cryptography and the imposition of secrecy orders upon papers it considered 'dangerous', amounted to an unconstitutional prior restraint on free speech, thus sacrificing a Constitutional right for national security.[9]

Attempts by the federal government to impose a mandatory key escrow system on encryption technologies also infringed on the Fifth Amendment right against self-incrimination. The key escrow system gave the federal government the ability to decrypt any data or communications encrypted using an escrowed system, even without the consent or cooperation of the individual(s) involved. Even if a criminal had encrypted incriminating evidence on his computer's hard drive and refused to give up his password or encryption key – a right guaranteed him by the Fifth Amendment – the government could still force disclosure of the information through the 'back door' provided by the escrowed key. Although this point is debatable, at least some critics believed that it granted authorities a means of circumventing the intent of the Fifth Amendment.

Civil libertarians and activists would seize upon the threat to civil liberties posed by the export controls as a rallying point. In general, as their ideological motivations pushed them toward the less restrictive encryption policies also favored by the software industry, the two would find common ground and cooperate in their lobbying efforts, thus uniting the ideological and populist appeal of the civil liberties lobbies with the money and political influence of the wealthy software industry.

### *The Debate: Encryption and Regulation from 1973-1999*

The significance of the debate over encryption policy lies in the values that were at stake. Each of these values, whether national security, economic interests, or civil liberties, plays an important role in American society, and the encryption debate forced policymakers to choose between them. For much of the period from 1973-1999, the national security argument trumped the others, even though external conditions, particularly the rapid advances in technology and computing, including encryption technologies, the popularity of the Internet, and rapidly improving computer processors, eroded the effectiveness and impact of export controls. By 1991, government policies imposed the costs of losing of civil liberties and economic benefits without producing the offsetting gains in national security. Not until 1999 would this imbalance be rectified through a shift in national policy.

[9] See Bernstein v. United States Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).

Export controls and other restrictions on encryption, particularly the International Traffic in Arms Regulations (ITAR), were developed during the Cold War and enforced by a variety of federal agencies and international efforts such as the Coordinating Committee for Multilateral Export Controls (CoCom).[10] Encryption technologies were heavily restricted during the Cold War, even though by the 1980s strong encryption products were available from foreign commercial sources, including U.S. allies who used the heavily restricted U.S. federal standard algorithms in their products. The products were not as accessible or user-friendly as they are today, but the technologies were available to anyone determined to obtain them.

It seems reasonable that those who the U.S. government most feared would obtain encryption were precisely those with the greatest incentive and means to do so, and implausible to argue that terrorists who could plan an airplane hijacking or criminals who could run an international drug-smuggling enterprise would be incapable of buying an encryption program from a supplier in Germany where it was commercially available. Alternatively, the same customer could purchase the identical restricted technology within the U.S., where it was not restricted, copy the program into his computer, and leave the country. [11] Again, it hardly seems plausible that export controls would pose a significant deterrent or obstacle to someone determined to have strong encryption. Thus by restricting U.S. exports of encryption technologies, the government served only to make it less widely available -- or, as the software industry argued, to force those who wanted it to buy from non-American firms.

When the computer software industry began its explosive growth spurt of the 1990s, government efforts to control encryption intensified, despite the fact encryption technology was widely available in at least 35 countries, from 455 different manufacturers.[12] In addition, aside from commercial sources, a freeware strong encryption program called Pretty Good Privacy (PGP) had launched in 1991 and almost instantly proliferated via the Internet to almost all corners of the globe, safely out of the reach of government control and thereby eliminating cost and access barriers to encryption. Nonetheless, the restrictions on encryption in place since the start of the Cold War were not lifted until 1999, nearly a decade after PGP, if nothing else, had rendered them functionally obsolete.

The export controls of encryption were not wholly ineffective or without benefit to national security, however, because the NSA had an interest not only in preventing hostile states and groups from obtaining encryption but also in limiting the amount of strong encryption in use. The encryption regulations did serve a few purposes. First, U.S. dominance in the computer software industry meant that

[10] In 1996, encryption regulation shifted from ITAR to the new Export Administration Regulations (EAR) under the Department of Commerce.

[11] The contents of hard drives are rarely if ever checked when leaving the country, and indeed countless American executives no doubt inadvertently violated export laws by leaving the country with their laptops containing encryption programs, before the 'laptop clause' was inserted into export regulations.

[12] Software Publishers Association, Worldwide Survey of Cryptographic Products (June 1995).

U.S. products were and would become de facto international standards. Building strong encryption into U.S. products would therefore make encryption more widely available even to consumers who would not otherwise have sought it out, or who might not even be aware of its presence but inadvertently use it. This would in turn increase the number of encrypted communications considerably. Before the 1990s, use of encryption was largely limited to the government, financial services, and government contractors, who used the federal encryption standard; large corporations, which used their own or the federal encryption standard (Digital Encryption Standard, DES); and extremely techno-savvy individuals, who frequently wrote their own or used ones developed by fellow computer enthusiasts. The number of people and organizations who actually encrypted their communications was quite limited, and the first group was considered 'safe', as they were vetted by the government prior to being allowed to use DES. Making encryption user-friendly and widely available meant anyone who did not fall into the previous categories could potentially also encrypt their communications, thereby complicating the work of communications intelligence.[13]

Second, because an export control regime is ultimately an international effort, the U.S. needed to comport itself as a standard for other countries to live up to. Since the U.S. had one of the most stringent export control policies on encryption and actively lobbied other countries to impose similar standards, it could not credibly do so unless it also adhered to those strict standards. Its insistence and example did help push Britain and Australia, if not other countries, to adopt somewhat stricter encryption policies, though it is debatable whether it was the overall relationship or the U.S.'s example that led to the changes. In general, attempts to pressure other countries to restrict encryption technologies ranged from moderately successful during the Cold War years to downright ineffective in the post-Cold War era. Many of the other major producers of encryption technologies simply did not view encryption as being as dangerous as the U.S. did; alternatively, they put a higher value of the principle of right to privacy. The U.S.'s many failed attempts to convince the international community to stricter encryption controls suggests that the government was aware that any success in international cooperation would fall far short of the U.S.'s own desired control policy.

Third, even though the export controls could not put the encryption genie back into the bottle, it could ensure that all new developments in commercial cryptography were sent to the NSA for review and approval, a cheap and easy way for the NSA to monitor progress in the field. Because exporters are required to disclose the details of their products to the government on a routine basis, though not

[13] However, the counterfactual is that adoption of a particular software or type of encryption as a de facto international standard might have made the NSA's job easier, because it would give them only one cryptosystem to break. If they could find a weakness in a particular encryption algorithm – and the export control review process would give them a head start in doing so since U.S. firms would pre-submit their products for review – they would be able to exploit it for a larger volume of communications, rather than having to find weaknesses in a half dozen other, non-U.S. programs.

necessarily to modify them to get an export license, it ensures that the NSA will know how each product functions, which presumably gives it an edge in cracking encryption done by that system when it is deployed.[14] Pre-publication review of cryptologic papers, too, allows easy monitoring of academic developments in cryptology, and if not abused by the NSA to impose secrecy orders, fosters goodwill toward the NSA among independent cryptologists who could potentially challenge NSA's expertise. Thus, export controls were not only the objective of the government but a logical step in the absence of better alternatives. The government lacked any other real options besides export controls and secrecy orders for preventing dissemination of cryptographic information and products abroad. It could not prevent companies in other countries from selling it, nor force foreign governments to do so. By the 1990s, it could not control the content of the Internet, either, as PGP proliferated on international sites. Though ultimately futile, the restrictions were the equivalent of one-man-against-a-flood philosophy – anyone stopped from using strong encryption was one more than before.

Fourth, the export controls may well have bought the NSA time to develop ways of defeating the new commercial cryptosystems. The NSA, with its vast banks of supercomputers, the highest concentration of mathematicians and cryptologists in the U.S. and possibly the world, and the immense resources of the federal government, is considered the world leader in cryptology and electronic communications systems. Even today its superiority to the civilian sector in cryptology is assumed, so it is not implausible that any amount of extra time could have allowed it to create and/or lock in its technological advantage against commercial systems and preserve its SIGINT capabilities. The NSA's history certainly suggests that it does not lie still in developing and exploiting new technologies: during the Cold War, it was one of the largest backers of research and development of microchips and supercomputers, and today, it is one of the largest backers of research into advanced mathematics, quantum computing, nanotechnology, networking technologies and computer systems security, each of which hold profound implications for the future of cryptology.[15] The problem, of course, is that there is no way to test this theory due to a lack of information, though the empirics certainly seem to fit.[16]

For the purposes of this study, then, the fundamental debate was a normative one. Were the marginal benefits of export controls – pre-publication review, slowing the diffusion of mass market encryption, setting an example for the international community – worth the costs imposed on the software industry and the damage done to civil liberties? How were these value judgments made, and by whom? And how did the change in policy, which if policies had followed the external environment would have occurred a decade earlier, finally come about in 1999?

[14] Whit Diffie and Susan Landau, *Privacy on the Line* (Cambridge: MIT Press, 1999), 107-8.
[15] See NSA website for past and current research areas. http://www.nsa.gov/research/index.cfm
[16] I would like to thank Steve Rosen for bringing up this point.

The significance of this case, more broadly writ, is in its implications for the ability of the U.S. government to regulate growing industries and industries with rapidly changing technologies. The control and eventual relaxation of controls of encryption technologies illustrates a case in which policymakers had difficulty changing a policy rendered ineffective by changing conditions, despite the high costs of maintaining that policy. National security arguments, combined with capture of critical components of government, allowed a costly and ineffective government policy to continue for almost a decade before policies were adapted to fit existing conditions.

### *Analytical Framework*

Theories of the political process attempt to identify factors that influence the making of public policy and explain the processes and outcomes. The ability and motivations of policy-makers to improve and adapt policies to fit changing conditions and technologies is a small part of this policy process, and will be a focus of this paper. Contemporary theories of regulation in organization theory, political science and economics all suggest that regulations usually change slowly, and that change is usually driven by powerful material interests, sometimes bolstered by a sense of impending or recent crisis. Both the political science and organization theory literature are pessimistic with regards to large organizations' ability to adapt effectively and quickly, but both also suggest that there are conditions under which it is possible.

My argument draws upon a combination of organization theory and the political science-economics literature on interest groups. Within organization theory, the literature on the formation of organizational interests and organizational culture sheds light on the motivations of the various government agencies, particularly the NSA, that helped shape the evolution of national encryption policy. The interest group literature helps explain how the national security establishment was able to maintain control over national policy even after the technological and political conditions in which the original policies were formed no longer existed. In conjunction with organizational culture, interest group politics accounts for the desire of the national security establishment to maintain policies even after they were no longer effective. The interest group literature also helps explain how opposing interest groups, namely the software industry and civil liberties activists, were able to organize and mobilize to lobby previously neutral members of Congress to effect a change in national policy over the objections of the national security establishment.

### *Political Science Theories*

The political science literature suggests that both the structure of the American government and the role of interest groups in the American political process limit the ability of the government to adapt its policies. Theories that focus on the structure of government note that separation of powers imposes significant transaction costs on policy change and creates multiple choke-points at which policy changes can be held up or stopped completely. These theories tend to emphasize the role of crises, whether real or perceived, and mobilization of public opinion as impetus for change. Interest group politics, on the other hand, looks to the concentration of interests as a determinant of successful policy change.

Structurally, the legislative process is designed to prevent rapid change, a legacy of the Founding Fathers who feared inconstancy of democratic rule. The process of bringing a bill to a vote is a circuitous one, with multiple detours through an assortment of subcommittees and committees and chamber leaderships, each of which can amend the bill and send it back to its starting point for reconsideration by all previous committees. In each stage, bargaining and coalition formation are necessary to ensure that the bill clears another legislative hurdle, thus raising transactions costs for all involved. Should the bill make it to a vote without being bottled up by a committee chairman or strategically placed minority of opponents, it must then obtain a majority of votes in both houses of Congress and avoid a Presidential veto.[17] Meanwhile, because legislation is only made and not executed or enforced by the legislative branch, the executive agencies that implement the legislation have considerable leeway in how they choose to interpret the legislation. Hence, legislation usually contains control mechanisms to ensure that legislative intent is exercised in the execution of the legislation, sacrificing flexibility in regulatory implementation and future adaptation for security of the current implementation.[18]

Given the barriers to change in the American system, mass mobilization is one of the few methods for rapidly bringing about policy change. Highly publicized policy failures that spark public discussion of an imminent or ongoing 'crisis' represent one of the few ways to circumvent the inertia of the policy process and spur policy makers into finding the causes and a solution to the problem. Policy

[17] For discussion of committee chairmen as legislative gatekeepers, see Richard Fenno, *Congressmen in Committees* (Berkeley: Institute of Governmental Studies Press, 1995). Ken Shepsle and Barry Weingast, "The Institutional Foundations of Committee Power," *American Political Science Review*, Vol. 81, No. 1 (March 1987): 85-104, argue that the conference committee enables committees to ensure that the views of the committee majority are incorporated into legislation, even when a majority in the legislature would prefer another outcome. I drew both references from Brian Zuckerman, "Long-Term Trends, Adaptation, and Evaluation in U.S. Regulatory Policy" (Ph.D. diss., Massachusetts Institute of Technology, 1993), Ch. 1.

[18] Mathew D. McCubbins, Roger G. Noll, and Barry R. Weingast, "Administrative Procedures as Instruments of Political Control," *Journal of Law, Economics, and Organizations* 3 (1987): 243-277. This collaboration argues that specifying procedures helps alleviate the principal-agent problems inherent in the legislative-executive relationship. First, it cuts down on the information asymmetry of agencies having greater expertise than legislators. Legislation such as the Freedom of Information Act reduces barriers to information for legislators and constituents, require explanation of the rationale behind new regulations, force incorporation of new information during redesign of regulations, and limit agency discretion in general by increasing transparency of agency actions and subjecting them to greater constituent oversight. Second, by designing specific procedures into legislation [i.e., not just telling agencies what to do but how to do it], legislators can influence the implementation and evolution of policy, to the extent of even favoring certain interest groups over others, allowing the policy to adjust over time without new legislation.

entrepreneurs may step into the breach to advocate a particular and often different policy solution that would have gone unnoticed or ignored without the crisis situation. Meanwhile, the crisis prompts a change in preferences, however transitory, of the supporters of the existing policies, prying loose entrenched interests that would otherwise prevent adoption of a new and different policy.[19]

The influence of interest groups on policy processes has received considerable attention in the social science literature as well. Within political science, pluralists argue that policies are the result of conflicts and compromises among organized groups, including parts of the government and non-government interest groups. Access to government officials, in particular, can influence the chances of success of a particular interest group's agenda.[20] The economists George Stigler and Mancur Olson each provide an explanation of role of interest groups, particularly industry, in the policy process. Stigler argues that industry can capture regulation and regulatory agencies such that regulation will be designed to lock in benefits for that particular industry or firm in the future.[21] These benefits can include regulation that limits entry and slows growth of new firms relative to existing ones, or favors existing products and complements to existing products while banning or restricting competing products. In exchange regulators receive electoral support and other perquisites.

Olson's theory of collective action focuses instead on the role played by concentrated interests versus diffuse interests. Olson argues that concentrated interests are overrepresented in the policy process because they have a strong incentive to organize and devote resources to effectively influencing the policy process. The smaller number of actors in the concentrated interests increases the share of benefits each stands to gain from successful political action. Diffuse interests, on the other hand, individually stand to gain comparatively little from successful action, even as the higher costs of organizing and mobilizing large numbers of participants increases the costs of action. Hence, Olson argues, diffuse interests tend to be underrepresented in the policy process.[22] Olson does suggest, however, that the obstacles to mobilization can be overcome if an individual or individuals have a social incentive (prestige, friendship, respect) that would bring them individual reward.[23]

[19] John W. Kingdon, *Agendas, Alternatives, and Public Policies* (Boston: Little, Brown, and Company, 1995).

[20] Earl Latham, *The Group Basis of Politics: A Study of Basing-Point Legislation* (New York: Octagon Books, 1965); David Truman, *The Governmental Process: Political Interests and Public Opinion* (New York: Alfred A. Knopf, 1953). Latham in particular argued that interest groups dominated the policy process, with the government facilitating compromise, serving as a referee in the conflict, and ultimately recording its outcome in the form of legislation or policy. Truman, on the hand, focuses more on access to government officials during the legislative and administrative (implementation) processes as an indicator of success in the policy process.

[21] George J. Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics*, Vol. 2, No. 1 (Spring 1971), 2-21, 3.

[22] Mancur Olson, *The Rise and Decline of Nations: Economic Growth, Stagflation, and Social Rigidities* (New Haven and London: Yale University Press, 1982), Chapter 2.

[23] Olson, *Logic of Collective Action* (Cambridge: Harvard University Press, 1965), 60-1.

Taken together, Stigler and Olson suggest that large concentrated interests will have their views disproportionately represented in regulation, and that they will resist changes that damage their established interests. However, the theories also leave open the possibility that another powerful interest group with sufficient mobilized public support could also successfully vie for position in the policy process.

*Organization Theory*

Shifting to the interests and behavior of organizations, the organization theory literature also suggests that adaptation should be difficult, albeit for different reasons. Organization theory suggests an organizational tendency to inertia as a result of the routinization function of all bureaucracies. As James Q. Wilson writes, organizations are created to "replace the uncertain expectations and haphazard activities of voluntary endeavors with the stability and routine of organized relationships."[24] That is, organizations rely upon standard operating procedures or routines to streamline their work. By their very nature, therefore, organizations should resist adaptation because it brings them back to their original state of confronting each problem as a new and discrete situation, thereby eliminating the efficiencies of having a standard operating procedure and the purpose of creating the organization. Crisis, therefore, plays an important role as a motivator of change in organization theory because the lack of operating procedures that address the current situation forces change. The threat to the organization's survival also reduces opposition of its members to innovation. Crisis, therefore, breaks down barriers within organizations to adaptation.[25] The alternative interpretation, however, is that organizations fixated on a particular mode of operation will instead refuse change in the face of crisis, seeing only limited options bounded by the walls of their own standard procedures, and thus fail to adapt.[26]

An additional factor contributing to organizational inertia results from operating under an unclear or conflicting mission, a situation that occurs frequently in government agencies. In such a case, the act of choosing one goal over another may disturb the power balance between factions of the organization.[27]

[24] James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989), 221.

[25] James Q. Wilson, "Innovation in Organizations: Notes Toward A Theory," in James D. Thompson, *Approaches to Organizational Design* (Pittsburgh: University of Pittsburgh Press, 1966), 194-219, 208; Aaron Wildavsky, *Speaking Truth to Power: The Art and Craft of Policy Analysis* (Boston: Little, Brown and Company, 1979), 217-218.

[26] Graham Allison. "Conceptual Models and the Cuban Missile Crisis." *American Foreign Policy: Theoretical Essays*. Ed. G. John Ikenberry. New York: Longman, 1999. 413-458.

[27] Graham Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: HarperCollins, 1971), 83; Wilson, Bureaucracy, 117, 375; Wildavsky, 215. Wilson cites the example of the Social Security Administration as being an organization originally created for one purpose – distributing social security checks to retirees – that was saddled with another task that clashed fundamentally with its organizational culture. When the SSA was also assigned the task of distributing disability checks, which required them to shift from a customer-service oriented

Hence in a factionalized organization or organization with many discrete subunits, the need to preserve the balance of power between factions may override a greater institutional need or ability to change.

*Organizational Culture*

The organizational culture literature within organization theory suggests an explanation for the motivations of an organization beyond pure material interest. Edgar Schein defines organizational culture as "the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[28] By extension, the assumptions that comprise organizational culture can become the personality and mission – not only in the sense of assigned duty, but of perceived objective – of an organization, and fundamental to its survival as a group or organization. As Wilson notes, an organization that has successfully imbued its members with a culture appropriate to their environment, "a rational definition of their core tasks," will be more successful than rival organizations that have not.[29] The role of culture in determining the organization's way of seeing and responding to the world becomes especially strong when the organization's stated goals are vague or very broadly written, as the culture becomes a set of guidelines for how to interpret and accomplish those goals.[30] The drawback, as with standard operating procedure, is that organizational culture can sometimes take on a life of its own and "blind the organization to changed environmental circumstances so that new opportunities and challenges are met with routinized rather than adaptive behavior. But even short of occasions for major organizational change, the perceptions supplied by an organizational culture sometimes can lead an official to behave not as the situation requires but as the culture expects."[31]

Schein argues that culture is formed through two types of learning situations: problem solving and anxiety avoidance. Both types provide immediate positive or negative feedback, depending on whether the solution to the problem works or whether the anxiety is successfully avoided. However, the latter type of learned behavior tends to remain in an organization longer, because if it works the first time, the anxiety-avoidance behavior will continue likely indefinitely because the organization will not

mindset to an evaluative mindset (is this person really disabled enough to receive benefits?), it wreaked havoc on the organizational culture and created conflicting goals.

[28] Schein 3. Schein argues that to fully understand a culture, one must delve into the underlying assumptions, which are often unconscious but actually determine how group members perceive, think and feel. These are often learned responses that originated as espoused values, which over time have transformed into underlying assumptions about how things really are. He cites as examples the notion that businesses should be profitable, schools should educate, or medicine should prolong life as examples of values that have become so deeply ingrained as to become assumptions.

[29] Wilson, *Bureaucracy*, 92.

[30] *Ibid.* 93.

[31] *Ibid.* 110.

willingly test the situation to see if the source of the anxiety is still operating, so that the behavioral adaptation will continue even when the situation no longer exists. In other words, anxiety-avoidance behavior is the organizational equivalent of the cat that will no longer sit on any stove lid, hot or otherwise, because it does not care to check whether the stove lid in question is hot or cold.[32] Problem-solving behavior, on the other hand, requires continual use and therefore provides continual feedback on success or failure, and the need for adaptation. Thus organizational culture theories provide an outlet for adaptation, in that as an organization develops, it may modify to some extent its original assumptions to adapt to the environment and ensure its survival – find its niche, in other words, without fundamentally altering its original objectives.

### *Autonomy*

Organizational theory also suggests another characteristic of organizations that bears on this case. Perhaps even more than economic benefits, organizations pursue autonomy, defined by Philip Selznick as the "condition of independence sufficient to permit a group to work out and maintain a distinctive identity."[33] Autonomy is sometimes referred to as 'turf', although per Wilson, it has both internal and external aspects. Internal autonomy relates to organizational culture in the form of organizational identity and mission, or the shared understanding of the central tasks of the agency. The external aspects of autonomy take the form of jurisdiction and domain; organizations seek to reduce bureaucratic rivals, and also to limit the amount of oversight or political constraints imposed by superiors. Organizations also seek to match jurisdiction and mission, meaning that they seek to ensure that their assigned tasks are in accord with their perceived organizational mission, and resist taking on missions that do not fit into their perception of 'self'.[34] As a consequence of the concern for autonomy, it is difficult to coordinate the work of different agencies. Government agencies view any interagency agreement as a threat to their autonomy and resist regulation by other agencies, such that coordination and cooperation, even when mandated or necessary for adaptation to changing conditions, are difficult.[35]

Thus, the political science and organization theory literature both suggest that adaptation will rarely occur, unless a crisis and/or a coalition of interest groups favoring change can pressure government agencies into making it more likely. In the absence of such pressures, the status quo will continue, even if shifts in the external environment make the policies ill-suited for existing conditions.

### ***Theory meets empirics***

[32] Schein 7-8.

[33] Philip Selznick, *Leadership in Administration* (Evanston, Ill.: Row, Peterson & Co., 1957), 121, in Wilson, *Bureaucracy*, 182.

[34] Wilson, *Bureaucracy*, 182-3.

[35] *Ibid.* 192.

In applying each of the political science and organizational theories to the encryption policy case, I take a broadly constructivist analytic approach. Constructivism postulates that interests are based upon ideas, and specifically common ideas shared by groups (intersubjective beliefs). Individuals and organizations, by extension, will act based upon these beliefs as though they are their interests, though they may run counter to conventional conceptions of interests.[36] In this case, the actions of each of the various players in the debate (NSA, industry, civil liberties activists) either stemmed from their beliefs and or formed the basis of their lobbying efforts. Each of the outcomes, whether the successful capture of critical Congressional committees by the NSA, the NSA's recruitment of allies in the national security establishment, or the software industry-civil liberties lobby alliance's successful conversion of previously neutral members of Congress and the public to their point of view, all relied upon creative and convincing argument. Although one could argue that organizational (or corporate) interest alone could motivate the NSA and software industries, it cannot account for their successful lobbying of their respective branches of government; the presidency and most of the Congressmen who eventually came to play the greatest role in reforming encryption policy had little or no personal stake in the issue.

Overall, the political science and organization theories are complementary with regards to the case of encryption policy. They make similar predictions about organizational inertia and the unwillingness of the government to change its policies, although the reasons differ: regulatory capture, the difficulty of organizing an opposition, desire for autonomy, reluctance to confront new anxiety-inducing situations, and organizational culture. In the following chapters, the role of each of these mechanisms is explored, as each has a role to play in the process and outcome of the policy debate.

*Expectations from Theory*

During the formative period of encryption policy, the dominant influence on policy was the NSA. As the acknowledged authority on communications intelligence and cryptology, and bolstered by the tensions of the Cold War that created an imperative to value national security interests above all other competing interests, the NSA was able to enact a strong, restrictive export control policy. (See Table 1.1 for summary of policy preference of the various actors.) The NSA also nurtured its cultural antipathy to publicity during this period, preferring to work behind the scenes and out of the public spotlight. Through argumentation in the form of Congressional and executive briefings, in which the NSA indoctrinated Congressmen in critical supervisory committees such as the Senate and House Select Intelligence committees and Foreign Relations/ International Relations committees and created a sense of belonging the exclusive club of the national security elite, the NSA was able to capture regulators by converting

[36] See Martha Finnemore, *National Interests in International Society*. (Ithaca: Cornell University Press, 1996), Ch. 1. for a very good explanation of the constructivist approach.

their interests to align with the NSA's own. These Congressmen, in turn, pushed the NSA's agenda through Congress, meeting with little resistance from their colleagues, who had little pre-existing interest in the issue. At this time, the software industry was in its infancy, and civil liberties groups were scarcely aware of the existence of encryption, much less the NSA.

As predicted by political science theories and organizational culture, the few times when the NSA's grip on export control policy was challenged were in the face of crises that received significant public attention. When an NSA employee sent a letter attempting to shut down a cryptography conference by warning of violations of export laws, and when the NSA tried to impose secrecy orders on two patent applications filed by independent researchers, the resultant media firestorm forced the NSA to retreat. Congressional investigations into encryption policy and the NSA's activities during this period were, with one exception, initiated by Congressmen who were not members of the NSA's captured committees. The one exception uncovered NSA projects to monitor American citizens, but because the investigation was conducted by the Senate Select Intelligence Committee, the NSA escaped with only a reprimand. The two other Congressional investigations during this period were focused instead on NSA's attempts to seize bureaucratic turf from another agency in violation of a Congressional act, and an attempt by the Presidency to seize policy-making initiatives from the Congress; neither actually focused on the encryption policies themselves.

Organization theories' predictions regarding organizational reluctance to cooperate with other agencies or share bureaucratic turf also held true during this period. Throughout the 1970s and 1980s, the NSA repeatedly tried to wrest the right to fund cryptographic research from the National Science Foundation (NSF), because it threatened not only the NSA's monopoly on cryptography, but because it could take away its pre-publication review rights. The NSA also found a way around Congressional legislation that granted the right to control civilian cryptography to another agency, the National Institute of Standards and Technology (NIST), thereby functionally preserving its self-assigned bureaucratic turf.

In the transitional period from 1991-99, the NSA's grip on the Presidency and key Congressional committees began to break down, challenged by the end of the Cold War, which reduced the strength of the NSA's national security argument, and the infusion of 'new blood' with a more liberal, economic-based platform in Congress. It was during this period that Congress and the public began to realize that export controls no longer provided the same benefits to national security that they had in the past, while the costs to the software industry, individual computer users, and civil liberties had risen. Only during this period did Congressional hearings on national encryption policy focus on the policy itself rather than threats to Congressional turf or authority. The hearings even began in the Foreign Affairs committee in the House, a traditionally 'captive' committee for the NSA, at the instigation of a new Congresswoman from Washington, home of the newly formed software industry and its political lobbyists. Notably, the

Subcommittee on Economic Policy, Trade, and Environment spearheaded the hearings, representing a shift away from national security and toward economics that marked the beginning of NSA's loss of influence over national encryption policy.

Table 1.1

| Actor | Preferred Encryption Policy (Strong or Weak restrictions) | | |
|---|---|---|---|
| | **1973-1991** | **1991-99** | **1999- present** |
| National security establishment (NSA, Intelligence/ foreign relations committees, Executive branch) | Strong | Strong | Strong |
| Software industry | N/A or neutral | Neutral or weaker | Weak |
| Civil liberties groups | Weak<br>N/A – not aware of issue | Weak | Weak |

This period also marked the formation and alliance of the software industry lobby and civil liberties groups to overcome Olsonian collective action problems, uniting the concentrated interests of the hard-hit software industry with the more diffuse but politically palatable civil liberties activists. In accordance with their organizational (or individual) interests, these groups favored weaker export controls on encryption technologies. They were able to appeal to the members of Congress without a pre-existing interest in the encryption issue and argue for a change in policy based on a different set of values (economics, civil liberties) than had previously grounded national encryption policy. They were also able to point to the shift in the national security-economics-civil liberties values tradeoff that technological improvements of the past decade had caused, further strengthening their case among Congressmen with more pragmatic concerns. The Congressmen they found to advocate their position were generally not members of the intelligence or foreign affairs committees in their respective houses. Although some of the advocates of policy reform were from regions with high concentrations of software firms (Silicon Valley, Washington state) that would explain their policy advocacy, the most influential and persistent advocates were actually from states with little or no constituent interest in the issue (Montana, Virginia) and whose political affiliations (conservative Republicans) on first glance should have made them opposed to liberal export policies.

The NSA, however, did not stand still during this period. It strengthened its position in government, recruiting other allies in the national security establishment and law enforcement to help argue its case for strong restrictions on encryption. The national security-law enforcement alliance, fronted by the FBI, then proceeded to lobby and capture the incoming Clinton administration through its presentations and warnings of the dire consequences of a failure to maintain a restrictive encryption policy. The NSA was thus able to not only advance its organizational interest but to do so in a way that fit in with its organizational culture, which required it to avoid the public spotlight as much as possible. The NSA also developed new tools for its policy toolkit, what Schein would term its problem-solving learning process, adding key escrow (the Clipper Chip and variants) to the already existing techniques of export controls, pre-publication review, and secrecy orders.

*Summary of External Environment for Cryptography and Government Actions (1973-1999)*

Table 1.2

| **Time Period** | **External environment (technological and political) for cryptographic technologies** | **Government actions** |
|---|---|---|
| 1970-1991 | Little to no mass market demand<br>Limited availability internationally<br>Small, weak software industry<br>No civil liberties lobbies<br>Little to no public awareness of encryption policies | Export controls<br>Federal Standards (DES)<br>Require cryptosystems to be in physical (chip) form<br>CoCOM |
| 1991-1999 | Mass market demand increasing<br>Strong cryptography widely available<br>Cryptography widely available in software form<br>Software industry growing stronger<br>Formation of civil liberties lobbies<br>Medium and increasing public awareness of encryption policies | Export controls continue or tighten, with a few minor liberalizations<br>Type I & Type II federal standards for cryptography, Digital Signature Standard<br>Key escrow/ Clipper Chip<br>Digital Telephony/ CALEA<br>Continue to require chip form<br>Wassenaar Arrangement (12/1998) replaces CoCOM<br>Transfer of export control authority from Department of State to Department of Commerce |
| 1999 - present | Strong cryptography widely available<br>Cryptography widely available in software form<br>Mass demand increasing/ high<br>Software industry fully developed<br>Strong civil liberties lobby; joined with software and other lobbies<br>High public awareness of encryption policies | SAFE bill, PRO-CODE introduced in Congress<br>Export restrictions eased through Presidential directive |

By 1996, however, the tide had turned against the NSA. A series of failed attempts by the Clinton administration to implement various encryption control schemes; the growing integration of computers and the Internet into daily life; failed attempts to elicit international cooperation in restricting encryption exports; continuous lobbying by a well-funded software industry lobby; rulings by federal courts that the export controls violated free speech; and a series of technological demonstrations by a group of dedicated civil libertarians-computer hackers of the weaknesses of current encryption technologies had turned public opinion, and by extension a significant portion of Congress, against the NSA and administration's preferred encryption policies. Several bills appeared in both houses of Congress that sought to revise existing encryption policy, and a report by the National Research Council refuted the NSA's argument that encryption policy could not be fully discussed without access to classified material and hence should not be a subject of public debate, stating instead that strong encryption should be made more widely available. In 1999, facing the likely passage of a bill that would reverse existing national policy and cut down existing export controls, the Clinton administration backed down and announced revisions in national policy that effectively eliminated restrictions on the export of mass-market encryption software. (See Table 1.2 for summary of empirics)

Table 1.3

| **Group** | **Preferred Policy Achieved** | | |
|---|---|---|---|
| | **1973-1991** | **1991-1999** | **1999-present** |
| National security establishment | Yes | Yes | No |
| Software industry | N/A or No | No | Yes |
| Civil liberties groups | N/A or No | No | Yes |

Table 1.3 shows the successes and failure of each of the groups involved in the debate over national encryption policy over the period 1973-1991. During the period from 1973-1991, particularly during the early half of that period, the software industry was just developing and encryption was so obscure an issue that it was not on the radar screen for civil liberties groups, which allowed the NSA to dominate national encryption policy. In addition, the dominant cryptography software producer for much of the 1970s and 1980s was IBM, which was itself an 'Establishment' company that willingly sacrificed potential profits (which were admittedly limited given the relatively small market for encryption software at the time) to further its relationship with the government, which was a major customer for its other divisions. By the late 1980s to 1990s, however, when the personal computer industry took off, and the

Internet explosion created a growing need and demand for cryptography, even IBM, which had by this time acquired Lotus, realized that the costs of adhering to the strict and largely ineffective export control policies were damaging their bottom line and, in their evaluation, incommensurate with the limited national security benefits they achieved. Lotus/IBM, along with the rest of the software industry, their allies in civil liberties groups, and libertarian computer enthusiasts spent the majority of the 1990s arguing the case for economic and civil liberties values over national security concerns. The national security establishment's influence on national encryption policy continued through most of this period, however, gradually weakening toward the end of the 1990s, until export controls were lifted in 1999, a policy that continues largely intact to this day.

### *Organization*

The next three chapters elaborate on the theories and issues presented above. Chapter 2 describes the formative period for encryption policy, from 1973-1991, and discusses the formation of the NSA and its organizational culture. Chapter 3 focuses upon the transitional period of 1991-99, from the release of PGP to the lifting of most export controls on cryptography. Chapter 4 concludes with a summary of the case and a discussion of some implications that can be drawn from it.

## Chapter 2

Each stage of the development of commercial encryption technologies from the 1970s to the early 1990s was marked by efforts by the NSA to restrict research on the development of those technologies. The NSA devised a number of strategies to suppress independent cryptographic research, control development and export of commercial encryption, and expand its influence and authority over encryption research and regulation. In each case, the NSA was fundamentally driven by a desire to protect its organizational interests in a manner consistent with its organizational culture, which emphasized secrecy and national security above all other interests. For the NSA, given its dual mission of COMSEC and COMINT, this took the specific form of maintaining superiority in its ability to perform its mission of obtaining and analyzing COMINT, and though expressed to a lesser degree in this study, creating secure ciphers (COMSEC).[37] The NSA's institutional aversion to publicity and its sense of the importance of its own mission were both products of its history, relics of the World War II signal intelligence agencies and wartime mentality during which it was created. The Cold War, with its accompanying political and military tensions, reinforced the NSA's belief in the importance of its work. The high priority given to the NSA's role by the rest of the government, combined with the NSA's successes, fostered organizational pride and an organizational culture focused on being and staying the best at cryptology—and on maintaining a monopoly on cryptology, which the NSA regarded as their exclusive area of expertise.

### *History of the NSA: Formation of Organizational Culture*

The NSA owes its existence to the failure of fragmented armed service intelligence agencies to adequately warn of the Pearl Harbor attacks and the start of the Korean War. During World War II, each of the armed services had their own cryptanalysis sections, but a lack of coordination between the services resulted in the warning of the Pearl Harbor attacks, which had actually been intercepted eight hours prior to the attack, not being delivered to the Pearl Harbor Navy headquarters until six and a half hours after the attack. Congressional investigations into the debacle and the pressures of coordinating burgeoning SIGINT traffic led to the establishment of a series of various coordinating bodies and agencies, ending with the Army Security Agency (ASA) in September 1945. Four years later, the newly formed Department of Defense secretly established the Armed Forces Security Agency (AFSA) to take over strategic communications-intelligence functions and coordination responsibilities of the various COMINT agencies, and added State Department cryptosystems to its list of responsibilities.[38] However,

[37] The NSA now calls this Information Assurance "IA", and the COMINT role is more specifically referred to as signals intelligence (SIGINT).

[38] Individual agencies retained tactical communications intelligence responsibilities, which are best done near the point of combat, and low-echelon communications security.

fragmentation of COMINT capabilities continued due to bureaucratic infighting, which led to another major intelligence failure: the failure to warn of the North Korean invasion of South Korea on June 25, 1950. The notice to target Korea for intelligence had, through bureaucratic miscommunication, had not reached AFSA despite the inter-agency oversight committee's ranking of Korea as the fifth most volatile area of the world. Hence not only did AFSA not warn of Korean invasion, it was not set up to handle Korean traffic once the invasion did take place.[39] The lack of warning of the start of the Korean War was deeply troubling to the Truman White House. The Secretaries of State and Defense jointly set up a commission to investigate COMINT resources and take corrective action. The Brownell Committee, as it would come to be known, issued a set of recommendations that were adopted almost in their entirety in the form of a Presidential directive issued in November 1952 that created the NSA, replacing AFSA.

The NSA's history and ancestry are thus rooted in war and wartime necessity. Born of agencies created to serve during WWII and the Korean War, it carried the wartime mentality with it into its formative years in the Cold War. The immediate transition from WWII into the Cold War, where a lack of communication between the U.S. and U.S.S.R. meant monitoring each others' actions depended heavily on signals intelligence, also meant that for the NSA, the war never ended. Operating under a wartime mentality created and sustained several quirks of the NSA's organizational culture that would prove problematic for those who wished to reform national encryption policy: a sense of the overriding importance of national security and the critical role the NSA played in preserving it; a habitual secrecy and secretiveness; and a sense of ownership over the entire field of cryptology.

First and foremost, the early history of the NSA ingrained into the organization the importance of national security and the critical role the NSA and communications intelligence played in preserving the American way of life. As the NSA's Security Education Program, an initiation and training program for new recruits, stated: "Our job with NSA is essential to the preservation of our American way of life. As part of that job, fulfilling our security obligations is equally essential to the success or failure of this Agency in the accomplishment of its mission.'[40] The lesson of the early years was that everything took a backseat to protecting national security. The NSA's belief in the importance of its own mission was not misplaced: during WWII, the cracking of German and Japanese diplomatic and military codes gave a significant advantage to the Allied forces, allowing them to anticipate at least some of their adversaries' diplomatic and military maneuvers. Admiral Chester Nimitz rated the value of COMINT in the Pacific as equivalent to another fleet; Gen. Thomas Handy "is reported to have said that it shortened the war in Europe by at least a year."[41]

[39] Bamford, *Puzzle Palace* 49-50.

[40] David Kahn, *The Codebreakers* (New York: MacMillan, 1967), 690.

[41] Bamford, *Puzzle Palace* 43.

After WWII, there was little evidence to refute the NSA's confidence in the supreme value of its mission, or its own impunity to law or punishment. If anything, how the rest of the government – or at least those who knew of the NSA's existence – treated the NSA probably only served to validate its own beliefs. National Security Council Intelligence Directive (NSCID) No. 9, a document dating back to July 1948 that had been renewed and updated to include the NSA in 1952, stated explicitly that COMINT be "treated in all respects as being outside the framework of other or general intelligence activities. *Orders, directive, policies or recommendations of any authority of the Executive branch relating to the collection... of intelligence shall not be applicable to Communications Intelligence activities, unless specifically so stated and issued by competent departmental or agency authority* represented on the [United States Communications Intelligence] Board. [italics added]"[42] What this meant was that, unlike every other individual and agency in the U.S., laws did not apply to the NSA *unless the law explicitly stated that it did.* It was the functional equivalent of a free pass for the NSA and other members of the COMINT community, and a situation that over time could quite understandably create sense of superiority, entitlement, and immunity from any restrictions. As James Bamford, the author of the first book on the NSA, wrote, "Despite its size and power, however, no law has ever been enacted prohibiting the NSA from engaging in any activity. There are only laws to prohibit the release of any information about the Agency."[43] The chairman of the Senate Intelligence Committee stated in an investigation into the NSA in 1975, "No statute establishes the NSA or defines the permissible scope of its responsibilities." [44] No other agency could make this claim – not even the CIA, which was established under the National Security Act of 1947, which set out the agency's legal mandate and restrictions on its activities.

The lack of restrictions on the NSA extended beyond even the legal carte blanche that NSCID No. 9 granted it. The very definition of COMINT was ripe for interpretation and abuse. The definition of COMINT was "intelligence produced by the study of foreign communications," but "foreign communications" was interpreted so broadly that it included anything coming from or going to foreign countries that "may contain information of military, political, scientific or economic value", by anyone who was a foreign national, agency, military, party, department, etc – or anyone who purported to work for them, regardless of citizenship.[45]

Nor did the traditional government check upon agencies, the budget process, exist. For the first twenty-five years of its existence, the NSA dominated the intelligence budget, but without anyone having real awareness of the scope of its budget or its activities, because its existence itself was so secret. Thus, after several decades, the NSA became accustomed to readily available resources and little supervision or

[42] Department of Justice, "Prosecutive Summary," March 4, 1977, p. 12, quoted in Bamford, *Puzzle Palace* 46.
[43] Bamford, *Puzzle Palace* 4.
[44] *Ibid.* 4.
[45] *Ibid.* 46.

oversight. Estimates of the NSA's portion of the intelligence budget ranged from 85-90%.[46] Given the lack of restrictions on the NSA's activities, carte blanche granted in the name of national security, it is small wonder that the NSA believed its mission and organization to be supreme in the hierarchy of national values.

The 1952 presidential directive that established the NSA charged it with the dual missions of maintaining the security of government information and gathering foreign intelligence. The structure of the NSA reflects this dual mission: the NSA has two divisions, Communications Security (COMSEC), which tries to devise unbreakable codes (cryptography), and Communications Intelligence (COMINT), which collects and decodes information from around the world (cryptanalysis).[47] For the first twenty years of the NSA's life, its mission – and even its existence—were rarely discussed publicly. Those who did know about it joked that the acronym stood for "No Such Agency". Access to the agency, located at Fort George Meade, Maryland, was severely restricted, and not just by the triple barbed-wire and electrified fence that surrounded its grounds.[48]

The second trait fostered by the wartime mentality dovetailed neatly with the national security considerations: secrecy. Due to the great value the government places on cryptologic material and the intelligence it provides, and as a function of the nature of the work itself, it follows that the NSA would have an organizational preference for secrecy. The Cold War, however, enhanced the sense of a need for secrecy, to the extent that the government did not even acknowledge the NSA's existence until five years after it was created.[49] It also ingrained the need for secrecy as an end to national security, but almost as an end unto itself, so deeply had the need been woven into the organizational ethos.

One way to search for organizational culture, writes Schein, is through analysis of the process and content of socialization of new members.[50] By this standard, secrecy undoubtedly occupied a prominent place in the NSA's organizational culture. As David Kahn, author of the first book to detail the activities of the NSA wrote: "NSA dins security security security security into its employees with remorseless

[46] United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Foreign and Military Intelligence,* Final Report, Book I, 94th Cong. 1st Session, 333-334, quoted in Bamford, *Puzzle Palace,* 2. See also Lee Lescaze, "Pentagon vs. CIA: Control of Intelligence Community Sparks Major Institutional Battle," *Washington Post,* June 10, 1977, A1; also quoted in Bamford.

[47] Although cryptography is only a part of cryptology, I use the terms interchangeably in this paper. Cryptology = cryptography + cryptanalysis. According to Bamford, *Puzzle Palace* 29, the term "cryptography" was until 1921 used to mean cryptography and cryptanalysis. The terms "cryptanalysis" and "cryptology" were coined by William Friedman, head of MI-8, America's first official cipher bureau.

[48] Bamford, *Puzzle Palace,* 88.

[49] The phrase "National Security Agency" first appeared in 1957 in the *United States Government Organization Manual.* Subsequent editions of the manual would have only the bland, set-phrase description "The National Security Agency was established pursuant to Presidential directive in 1952. It is an element of the Department of Defense, and its activities are subject to the direction and control of the Secretary of Defense." See *Government Operations Manual,* p. 204, in Kahn 675.

[50] Schein 3.

persistence until it becomes more than habitual, more than second nature—it becomes virtual instinct. Many, perhaps most, NSAers never tell their wives and children just what their jobs are. 'NSA,' they explain, stands for 'Never Say Anything.'"[51] The introduction of a handbook given to new NSA hires states: "By joining NSA you have been given an opportunity to participate in the activities of one of the most important intelligence organizations of the United States government. At the same time you have assumed a trust which carries with it a most important individual responsibility – the safeguarding of sensitive information vital to the security of our nation."[52]

Events during the formative years of the NSA would only underscore the need for secrecy and avoidance of public exposure. The agency's first two bites of the publicity apple undoubtedly left a bad taste in its mouth. The NSA made its public debut on the front page of the *New York Times* and *New York Sunday News* three years before the government formally acknowledged its existence.[53] On October 10, 1954, the *Times* reported that Joseph Sidney Petersen, Jr., an analyst at the NSA, had taken secret and top secret classified documents from his job and given them to a Dutch friend who he had met while working at AFSA during WWII. He had also shown copies of top-secret notes indicating that the U.S. had broken Dutch diplomatic codes to another Dutch friend.[54] Although Petersen was given a seven year sentence after agreeing to a plea bargain – meaning that the government managed to avoid the embarrassment of a trial and deter future offenders at the same time – it was a bitter experience for the NSA.

The second case was far more spectacular and public. In 1960 two American cryptologists, William Martin and Bernon Mitchell, defected to Soviet Russia. Kahn's account of their defection drily

[51] Kahn 690. Although this was written in the 1960s, I have heard anecdotal evidence that shows that this particular aspect of NSA culture still exists today. A friend whose Harvard physics lab is largely funded by the NSA related this amusing anecdote: several NSA representatives came up to Cambridge to visit the lab for a yearly review. One of the Harvard researchers, who had apparently been running a computer program that required a lot of processing power, remarked in an off-hand way, "I bet you have computers down at NSA that could process this so much faster," or something to that effect. The NSA representative replied, with a perfectly straight face, "I cannot confirm or deny that we have computers at NSA."

[52] Levy, *Crypto* 14.

[53] "U.S. Security Aide Accused of Taking Secret Documents," *New York Times,* October 10, 1954, pg. 1.

[54] Petersen had taken documents from his time at AFSA and at NSA, copies of the *Chinese Telegraphic Code* (secret) and a document on the routing of North Korean political traffic (top secret). He claimed that he had taken the documents home to help prepare lessons on cryptology for the instruction course he taught to new NSA recruits. It does not appear that Petersen had any malicious intent, but was rather careless of security precautions. His transfer of the documents to his Dutch friends, too, seemed genuinely motivated by a desire to help the Dutch – American allies – improve their cryptography. Both of the Dutch friends with whom he met and corresponded were friends dating back to Petersen's days at AFSA, where they worked side by side. Presumably, Petersen assumed that since they were privy to top secret information during the critical days of the war, they would still not be considered a national security threat after the war. The Dutch government, which acknowledged that Petersen had been passing information along to its agents for years, had thought Petersen was operating on the instructions of his superiors. In any case, by all accounts he seemed genuinely remorseful of his actions and did his best to repair the damage he had done – including agreeing to what was considered a very harsh sentence given his cooperation. See Kahn 690-2. See also Anthony Leviero, "Dutch Say Petersen Gave Data, But They Thought He Had Right," *New York Times,* October 20, 1954, p. 1.

notes, "[within] 90 minutes of blabbing at a Moscow press conference in 1960 [the defectors] told more to a bigger audience in less time about any nation's intelligence effort than any other traitors have ever done."[55] The subsequent media and Congressional investigations discovered blatant security breaches at the NSA. Both men were supposedly members of the Communist party; both had traveled to Cuba in violation of U.S. directives. Mitchell was probably a closet homosexual (then considered grounds for dismissal). The net result of their defection – and exposure of American cryptanalysis efforts – was that many nations had to change keys and systems, including the U.S.. President Eisenhower branded them traitors. The House Un-American Activities Committee, a special subcommittee of the House Armed Services Committee, and the Pentagon all launched investigations.[56] Needless to say, it was a public relations (and security) disaster for the NSA.

Theories of organization culture argue that experiences and lessons learned during the formative period can become behaviors that continue indefinitely, particularly if they help to avoid anxiety-inducing situations. Whereas secrecy had been a problem-solving behavior and therefore more easily adaptable before the two public security breaches, afterwards, it became a top-priority anxiety-avoidance response for the NSA. As Schein reasons, anxiety-avoidance behaviors continue because the organization does not wish to test the environment to see if the anxiety-inducing situation still exists, lest it be forced to confront it again. For the NSA, the Martin and Mitchell defections and anything associated with them were traumatic events to be forever burned into the organization's collective memory as a 'never-again' occurrence.

The third legacy of the wartime years was the NSA's belief that all cryptology was within its purview. During WWII and the first two decades of its existence, cryptology was functionally the exclusive domain of the NSA. Although it did not have a mandate that granted it authority over civilian cryptography, the fact was that cryptography simply did not exist outside of the NSA. The agency withheld information regarding cryptology from public view, and recruited and employed all of the mathematicians working on cryptology, thus drawing them behind the walls of federal classification and disclosure rules. It swallowed all papers and inventions sent for its perusal by would-be inventors, never acknowledging their receipt or possibly even their use, since security prevented the inventors and outsiders from ever finding out.[57] It also monitored all patent requests concerning cryptography, and used its authority to classify any that it deemed too powerful or too dangerous for release into the public domain. The NSA "considered itself the sole repository of cryptographic information in the country—not just that used by the civilian government and all the armed forces, as the law dictated, but that used by the

[55] Kahn 692.
[56] Account taken from Kahn 695.
[57] Kahn, quoted in Levy, *Crypto* 15.

private sector as well. Ultimately, the triple-depth electrified and barbed-wire fence surrounding its headquarters was not only a physical barrier but a metaphor for the NSA's near-fanatical drive to hide information about itself and its activities. In the United States of America, serious cryptology existed only behind the Triple Fence."[58] Thus, there was no one to contradict the NSA's view that it 'owned' cryptology. The troubles would begin in the late 1970s, when independent cryptographers working outside of the NSA began to challenge the NSA's monopoly.

In its first twenty years of existence, very little information on cryptography escaped the NSA's restrictions, with the exception of the Martin-Mitchell defections and the publication of David Kahn's 1000-page tome *The Codebreakers* in 1967, an event that the NSA had tried very hard to prevent. The book contained the first public account of the extent of the NSA's powers, carefully pieced together from bits of information that had leaked out in the prior decade. More importantly, though, the book contained a methodical explanation of the rules of cryptography and how the NSA used it: "the most complete description of the operations of Fort Meade that had ever been compiled without an EYES-ONLY stamp on each page."[59] James Bamford's *The Puzzle Palace* noted that the NSA had devoted "innumerable hours of meetings and discussions, involving the highest levels of the agency, including the director... in an attempt to sandbag the book."[60] Options ranging from purchase of the copyright to a break-in of Kahn's home were considered. Kahn himself, now living in Paris, was placed on the NSA's watch list, and his communications monitored. When Kahn's editor sent the manuscript to the Pentagon for review, it was forwarded to the NSA, and the publisher was told that publishing *The Codebreakers* "would not be in the national interest."[61] The NSA's director, Lt. Gen. Marshall Carter, then took the unprecedented step of meeting with the chairman of the publishing house, its lawyers, and the editor. Apparently, after attacking Kahn's reputation and expertise, the director then made a personal appeal for three specific deletions, which Kahn later granted. The book, with a statement that it had been submitted to the DOD for review, was finally published in 1967. It would not, however, be the last time NSA would try to prevent the spread of information on cryptography.

*DES (Digital Encryption Standard)—Trouble from the Start*

In May 1973, recognizing the need for cryptographic protection as computers became more important, the National Bureau of Standards (NBS) printed a solicitation for a standard cryptographic algorithm in the *Federal Register*. The Privacy Act of 1974 and other federal laws, when viewed in light

[58] Levy, *Crypto* 15.
[59] Levy, *Crypto* 23.
[60] Bamford, *Puzzle Palace* 168. Actually, in the early 1980s, the NSA would try to do suppress the publication of Bamford's *The Puzzle Palace* as well. (Mentioned in Diffie and Landau 231.)
[61] From Levy, *Crypto* 23.

of increasing use of computers, implied that approved cryptography must be available to government users other than NSA's traditional national security clients.[62] It initially received no acceptable proposals, probably since the only cryptographers who were capable of creating such an algorithm worked for the NSA. The NSA, despite the part of its mission that tasked it with maintaining the security of government communications – which included creating ciphers for federal use – refused to submit an algorithm of its own on the grounds that allowing outsiders to evaluate and examine its work would constitute an unacceptable threat to national security, as it might reveal information about the NSA's cryptographic design philosophy and potentially compromise other equipment.[63] The NSA would eventually come to regret this decision, when the non-NSA algorithm (DES) that was eventually approved became more widespread; thirteen years later, it would try to replace the DES algorithm with one of its own.

The algorithm that eventually did become the federal Digital Encryption Standard (DES), and by extension the *de facto* standard for private industry and individuals, began its life as the Lucifer cipher in one of IBM's research labs.[64] The Lucifer cipher and its product version were originally designed for Lloyds Bank in London to secure their automated teller machines (ATMs) against telephone fraud.[65] Lucifer was a block cipher that utilized sixteen rounds of substitutions, or 'rounds' of swapping letters with other letters in the alphabets, to ensure structural strength that would prevent detection and exploitation of subtle patterns in the encrypted text that would allow recovery of the plaintext without having to crack the encryption key.[66] The two 'substitution boxes' were essentially a set of complex nonlinear equations that contained the instructions for how letters would be shifted. These substitution instructions combined the letters with the digital key (a series of numbers) that comprised a secret set of instructions for how to vary the sequence. Thus the key was the basis of the security of the system. Without the key, even someone who knew Lucifer's substitution rules would not be able to reverse-

[62] See Diffie and Landau 59 and his footnotes. Notably, the law made no mention of individual or private users, only of government users.

[63] See Diffie and Landau 59 for rationale.

[64] The Lucifer cipher was an improvement on an earlier cipher written by Horst Feistel, the rather uncreatively titled "Demonstration." However, computer systems at the time did not allow such long file names, so it was shortened to "Demon". As a cryptographic pun, its successor was thus named "Lucifer".

[65] The ATMs were controlled through modems, so the phone service was vulnerable to a phone hacker who could get access to the phone line, dial the mainframe computer that controlled distribution of cash, and send a message saying, "Send me all your cash!"

[66] The basic principle of cryptography, or the writing of ciphers, is to produce a set of operations – an algorithm – that will create an end product that appears completely random. The lack of randomness, or the existence of even the subtlest of patterns, gives cryptanalysts a means to determine the original plaintext content of the message. For example, consider a simple cipher where letters are merely shifted one place, such as A=B, B=C, C=D, and so on. Frequency analysis of a relatively long message or set of messages would reveal that the letter "F" appeared most frequently, which in the English language would, based on the frequency of usage of various letters, mean that "F" probably stood for the letter "E". Continuing this analysis for each of the other letters, until a pattern of substitution was detected, would quickly reveal the cipher – and the plaintext of all future messages encoded with this cipher.

engineer the plaintext.[67] Knowledge of the substitution rules for widely distributed commercial ciphers was assumed, since they were likely to be far better understood than a government or military code, which could be more tightly controlled. Thus for non-military crypto, the key would provide all of the secrecy and security.[68]

Development of the DES system (officially called DSD-1 by IBM, but informally referred to still as Lucifer) took place over the course of several years after IBM first submitted it to NBS. It strengthened Lucifer to eight substitution boxes and 16 rounds of transformations (permutation, blocking, expansion, bonding, and substitution with a digital key, repeat 15 times) to create an apparently random block of digits that would hopefully be irreversible without the digital key. Testing by teams of IBM researchers and teams from the academic community continued for months, and no one succeeded in breaking the cipher. IBM feared for the security of its system – not because of the cost replacing cash to Lloyds, which IBM could easily afford, but because of the damage it would do to IBM's reputation.[69]

It was early 1974 when NSA contacted IBM to propose a quid pro quo re Lucifer. NSA gave IBM its list of demands: control of the implementation of the system, secret development of the project, the right to monitor progress and suggest changes, and shipment in chip form only (not code). It also informed IBM that it would restrict shipment of the chips to certain countries altogether,[70] and that the chips could be exported only to approved countries, and only with a license, obtainable only with a signed document from the customer promising not to re-export or re-sell the product. In exchange, NSA's cryptanalysts would test the algorithm to ensure that no weaknesses existed or remained in the system – thereby giving the product the NSA's quality certification.

In addition to imposing these conditions on the development of Lucifer, one of a series of export controls and other restrictions, the NSA also prompted the government to issue a secrecy order on Horst

[67] Lucifer, in several versions, was the brainchild of a German-born cryptographer named Horst Feistel working in IBM's research division in Yorktown Heights, NY. During WWII, Feistel worked on IFF systems. Feistel's greatest contribution to crypto may be his 1973 *Scientific American* article, which was not only the first time an unclassified article had laid out an explicit explanation of how a crypto system worked. It also detailed his motivation behind the project – not national security, but individual privacy. Feistel feared computers would allow for the theft of databases of personal information, enabling compilation of detailed dossiers on an entire population. See Levy, *Crypto* 41, and Horst Feistel, "Cryptography and Computer Privacy." *Scientific American.* Vol. 228 (May 1973). No. 5. pp. 15-23.

[68] In truth, there is an ongoing debate over whether open or secret ciphers are more secure. Advocates of secret ciphers argue that not knowing the algorithm creates an additional level of difficulty because it gives no hints on how to attack the cipher. This is not entirely true. A secret algorithm is only more secure in that *if the algorithm is somehow already flawed, as most are, and therefore vulnerable to attack, not knowing the algorithm slows down the rate at which the weakness will be discovered.* It does not actually make the algorithm more secure for practical purposes. The benefit of an open algorithm is that public debate and constant challenges from a community of cryptanalysts will reveal any design flaws faster, so that the algorithm can either be fixed or discarded before others find the same flaw and exploit it.

[69] Levy, *Crypto* 48.

[70] These states included the seven pariah countries: North Korea, Libya, Cuba, Iran, Iraq, Sudan, Syria.

Feistel's Lucifer patent, which made it a federal crime to publish on or publicly discuss Lucifer without written permission from the Commissioner of Patents.[71]

The costs generated by NSA's involvement in producing DES were not limited to the inconveniences of secrecy orders and export orders, however. During the process of putting Lucifer onto a chip, the original 128-bit key size was cut down to 56 bits, arguably a blow to the right to privacy. There continues to be some debate as to why this happened. Walter Tuchman, who headed up the product development at IBM for DES, insists that it was a combination of limitations of chip manufacturing, which could only fit 64 bits, and IBM's own (admittedly arbitrary) standard design practice, which required that 8 bits be left for system checks (parity checks). Functionally, what this meant was that the key was a binary number with 56 places. Although $2^{56}$, the number of possible combinations, is a large number, critics such as Marty Hellman and Whit Diffie, the two inventors of public key cryptography, argued that it was not a long enough key for strong encryption. A 56-bit key was still vulnerable to a brute force attack, [i.e., trying out the billions of possible combinations at lightning speed on a very fast computer or computers.] As Hellman put it, "A large key is not a guarantee of security, but a small key is a guarantee of insecurity."[72] Cutting Lucifer's original 128-bit key to 56-bits made it, mathematically speaking, $2^{56}$ times easier crack – that is, 70 quadrillion times easier.[73] Hellman and Diffie, in their critique, postulated that a 56-bit key could be broken in a day by a sophisticated, fast computer. They estimated one could be built for $20 million at the time, which at one key per day for five years meant the cost of breaking each key was about $10,000. IBM's own estimates were in the same ballpark.[74] This, however, did not factor in Moore's Law, which states that computer power doubles every 18 months, which would drastically reduce the amount time needed to crack each key, given a fixed 56-bit key length. That is, what took a day in January 1974 would only take 12 hours by June 1976, and 6 hours by the end of 1977.

An alternative explanation for the shortened key length emerged in the Senate Intelligence Committee hearings on DES that were sparked by the outpouring of public criticism of DES, including suspicions that NSA had inserted a 'trap door' in the system. The unclassified version of the report indicated that NSA was responsible for convincing IBM to use a reduced key size, because it would not tolerate anything more, despite still requiring export licenses even for approved customers. The NSA, which was working with NBS to evaluate DES as a government standard, had a strong incentive to cut the

[71] In an illustration of just how restrictive secrecy orders were, a special exemption had to be granted to the IBM researchers working on the system to allow them to continue their work; without it, even acknowledging the project's existence was an offense punishable by imprisonment.

[72] Whitfield Diffie, "Preliminary Remarks on the National Bureau of Standards Proposed Standard Encryption Algorithm for Computer Data Protection," May 1975, quoted in Levy 38.

[73] Account of DES and Lucifer drawn from Chapter 2 of Levy, *Crypto.*

[74] Levy, *Crypto* 58-60.

key length down. Although 56-bits would still require quite a bit of computing power to crack in a brute force attack, it was still short enough that, if anyone could do it, it was probably the NSA itself, which most people assumed had more and more powerful computers than anyone in the world.[75] Thus, by advocating a 56-bit key, the NSA could simultaneously appear to be fulfilling its COMSEC mission, while preserving its COMINT capabilities as well. As suggested by Wildavsky, in the face of unclear or conflicting goals, such NSA's mission of promoting both cryptography (COMSEC) and cryptanalysis (COMINT), an organization may simply make its decisions on the basis of maintaining the power balance between factions within the organization.[76] If it is true that the 56-bit key advocated by NSA emerged because it was a compromise between the COMSEC and COMINT factions within the NSA, it was also the last time that COMSEC prevailed. After DES, almost all of NSA's public cryptographic efforts would be toward suppression of cryptography.

*DES, The Aftermath*

The shift to emphasis on COMINT and preserving the NSA's cryptanalytic capabilities after DES was adopted would seem to be a product of the unexpected popularity of DES. Certification of DES created a monster that would forever change the environment for NSA's COMINT branch. First, creating a federal standard increased public awareness of cryptography, and the demand for strong cryptography soon spread beyond conservative institutions like banks and financial clearinghouses and found its way into commercial and even private communications. NSA's authority did not extend to monitoring domestic communications, and First Amendment issues prevented the restriction of domestic use of cryptography.[77] Second, although it controlled exports of the DES chips, in the years following certification, the algorithm itself found its way overseas, and was used by foreign developers to make their own versions of DES. Thus, its export controls were rendered functionally useless, as DES was readily available in a foreign-made version. Moreover, improvements in computer technologies meant that users could soon change keys every day, or even several times a day, making it even less likely that a broken key would lead to much lost information. To compound the problem, users soon figured out – as IBM had pointed out while trying to defend itself against accusations of producing a weakened product – that data could simply be encrypted several times. That is, they could run the data through the substitution boxes several times in succession, essentially re-encrypting already encrypted data so that, for the Triple

[75] Levy, *Crypto* 63.

[76] Unfortunately, though the unclassified facts of the case seem in accord with the predictions of the theory, I cannot find any evidence to suggest or refute the idea that there was a factional struggle within the NSA. An example of this argument can be found in Aaron Wildavsky, *Speaking Truth to Power: The Art and Craft of Policy Analysis* (Boston: Little, Brown and Company, 1979), 215.

[77] During Senate Intelligence Committee hearings in 1975, an NSA effort to monitor domestic communications, named "Project Shamrock", was revealed and roundly criticized by the Committee.

DES variant that emerged a few years later, decoding each message would require breaking *three* keys rather than one.

Widespread strong encryption presented a significant threat to the ability of NSA's COMINT branch to perform its mission. According to David Kahn's *The Codebreakers,* the first step in the process NSA uses to filter and analyze the vast number of communications it intercepts is similar to a keyword search.[78] For example, the DOD or another government organization tasks the NSA with finding out everything possible on, for example, sales of small arms to Sudan. The NSA would then program its computers, which continually monitor as much of the world's communications as it can intercept, to pull every message that contained certain keywords or names that analysts believed might appear: "Sudan," "AK-47", etc. These filtered communications would then be read and analyzed. Thus gathering and analyzing SIGINT requires that all communications be readable. With the use of strong encryption, this was no longer possible. By their very nature, encrypted communications in streaming form, whether encrypted with strong or weak encryption, look like gibberish and are not subject to such 'keyword searches'. However weak, the encryption must be decoded to obtain plaintext, which is tedious and time-consuming at the very least, and extremely difficult to impossible in the case of strong encryption. The cost (in time or resources) required to decode every single message, which would not have been necessary in a time of unencrypted communications, is prohibitive, increasing the chances of missing a critical message or piece of intelligence. This may be especially relevant when viewed in the context of the era, when it was believed that American and Soviet cryptography had evolved to such an extent that the respective intelligence organizations no longer even attempted to break each others' codes, instead focusing on the (frequently unencrypted) communications of their Third World allies to reveal intentions and information on their adversaries.

It seems likely that the NSA soon realized that explicit control of encryption was no longer possible. The encryption genie was out of the bottle. Rather, the goal became slowing the widespread deployment of cryptographic systems that could not be broken quickly or in real time by intercept equipment, which would render them functionally the same as plaintext – searchable. Therefore, the NSA's attempts to prevent adoption of cryptographic standards (in addition to its efforts to restrict use of cryptography, period) probably served dual purposes: 1) reducing likelihood of use of encryption, since adoption of a standard would increase use of cryptography, and 2) making sure that all messages didn't start to look alike, because they were all encrypted using the same unbreakable or difficult to break algorithms, because this would make them more difficult to distinguish from one another and therefore more difficult to scan.[79]

[78] See Kahn, chapter on NSA.
[79] Diffie and Landau 105-6.

While it is possible to target specific sources of data (particular email addresses, phone numbers, etc.) if they are encrypted, it requires cracking their encryption key to read the plaintext, an incredibly difficult task if the algorithm is well written and the key long. In addition, if the communications chain is kept anonymous, as in the case of anonymous e-mail remailers (especially if used in a chain, in tandem with encryption) that became popular after the 1980s, it may not be possible to trace even the origins of a particular email. While NSA may have found ways to deal with these problems, undoubtedly the development of these technologies has complicated its work exponentially. In time, elements within the NSA would come to see approval of DES, which would become common within U.S. borders, as a "horrible mistake."[80]

Another aspect of the DES development process that may have sparked NSA's increased sense of urgency in preventing the spread of cryptography and cryptographic information was the discovery that IBM's research team had independently discovered a cryptanalytic technique called the T attack, a type of differential cryptanalysis. This powerful technique was well known but highly classified behind the Triple Fence, and the fact the IBM researchers had not only discovered the technique but designed their S-boxes to defend against it unnerved the NSA. Shortly after the NSA reviewers working with the IBM found out about the re-design, they increased the security attached to the project, classifying every single document produced by the team. It was the greatest fear of NSA – that, because cryptography and cryptanalysis was essentially knowledge based, eventually, no matter how much information was classified, the same techniques and ideas would be discovered outside NSA. As an NSA official was to remark to Diffie at Crypto '82, "It's not that we haven't seen this territory before, but you are covering it very quickly."[81]

### *Public Key and RSA*

Soon after DES was adopted as the federal standard, two independent cryptographers named Whit Diffie and Marty Hellman revolutionized the world of cryptography with the discovery of public key cryptography.[82] One of the inviolable rules in the crypto world until then had been the concept of a symmetrical key: the same key used to encode was also used to decode, such that the security of the system depended upon the security of that key. However, this also meant that unless the sender and recipient had somehow met before, while the sender could easily encode the message, the recipient could

[80] Levy, *Crypto* 156.

[81] Diffie and Landau 239.

[82] In truth, although the discovery of Diffie-Hellman key exchange, or public key cryptography, is attributed to Diffie and Hellman, it was actually discovered some years earlier during the 1960s by a British cryptographer named James Ellis, who worked for the General Communications Headquarters (GCHQ), the British counterpart to the NSA. However, secrecy requirements prevented him from disclosing this discovery, and it remained a secret for almost thirty years. For a full account, see epilogue of Levy, *Crypto*. See also Levy, "The Open Secret," *Wired*, April 1999, and Simon Singh, *The Code Book*.

not, without the key, retrieve the message. In order to communicate securely, then, keys had to be passed from person to person, at minimum existing in two places. This dramatically increased the possibility of compromise.[83] For a military organization, it might be possible to protect that distribution, assuming no slip ups in the process, but for commercial purposes, with its large volume of communications, key distribution of symmetrical keys would be an enormous logistical, bureaucratic and security hassle. The key distribution center, too, presented a natural target for those seeking to break encrypted messages, and therefore a security risk.

Public key cryptography eliminated the problem of secure key distribution. It enabled users *who had never met* to communicate securely with a reasonable degree of certainty of the origin of the message. That is, it performed both encryption and authentication functions. It accomplished this by splitting the key, so that one half was public and the other private (and held only by one person). Each half of the key could decrypt the encryption performed by the other half. The use of one-way functions, mathematical functions that were easy to perform and near-impossible to reverse without a critical bit of information (the key), made this possible. For example, if Alice wanted to send a message to Bob, she would look up Bob's public key, encrypt her message using that key, and send it. Even if Eve, an eavesdropper, were to intercept the message, she would not be able to decode it because only Bob has the other (private) half of the key pair that can decode the message. For message authentication, Alice could also encrypt the message using her own private key. Bob, having received a message from 'Alice', would verify it was indeed from Alice and not some interloper by looking up Alice's public key, and decrypting the message. If a plaintext message emerged, then Bob could be reasonably certain the message was indeed from Alice. Because the actual text of the message is so deeply (mathematically) interwoven with the private key used to encrypt the message, the system also assures the integrity of the entire message, so that interlopers could not change even small bits of the text of the document from, for example, "I will not pay Bob's expenses" to "I *will* pay Bob's expenses." It functioned, essentially, as an un-forgeable, undeniable (because the encryption could only be done by someone with the private key) signature.[84] It was the discovery of public key that today makes official transactions – contracts, receipts, etc. – possible. Of course, the security of this system ultimately relied upon the security of the private keys – which were now safer because they were in the possession of one, and only one, person.

[83] The only truly secure system of cryptography, even today, is the one-time pad. Essentially, this is a system uses each key only once, so that breaking the key would not yield any information beyond a single message. The complications of this system should be obvious: it requires a huge amount of prior coordination between the two parties. In fact, it was such a hassle that it was only used for the most top-secret of communications during WWII – those between Churchill and FDR.

[84] In cryptography, the convention is not to use Person A, B, C, to denote sender, recipient, etc. Rather, following a quirk of the original RSA paper, each of these characters now has names: Alice the sender, Bob the recipient, Eve the eavesdropper, Carol, Dave, Trent, Wiry, and so on.

The concept and some basic ideas for implementation were published in an article called "Multiuser Cryptographic Techniques" by Diffie and Hellman in the journal *IEEE Transactions on Information Theory* in 1977. The two authors also continued to discuss and present their ideas at conferences both in the U.S. and abroad. In the article, the authors expressed the hope that this represented a "revolution in cryptography", and that their efforts would "inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly."[85]

The IEEE paper sparked the creation of what is quite possibly the widely used and best known cryptographic algorithm in the world: RSA, named for its three inventors, Ron Rivest, Adi Shamir, and Len Adleman, all professors at MIT. The IEEE paper had fallen short of actually creating an implementation that could be used. One of the problems remaining was the digital signature – namely, creating an actual, usable mathematical system with sufficiently powerful one-way functions. The solution Rivest eventually came up with was based on factoring, the breaking of composite numbers into their component primes. The public key would be the product of two very large prime numbers (each over 100 digits), combined with an encryption key consisting of another large number with certain properties. An encryption algorithm was added to transform the plaintext into ciphertext. The decryption key (the private key) was essentially an algorithm that could only be calculated only if one had the two original primes. Because of the difficulty of factoring, the public key, whose main component was just the product of the two primes, could be safely broadcast; until someone figured out an easier way to factor very large numbers – which after 2000 years, even the greatest mathematicians, from Eratosthenes to Fibonacci to Euler and Gauss, had not been able to do. The private key could also work in reverse, as an encryption key to be decoded by the public key, again because of the difficult of factoring – thus satisfying the requirements spelled out in the Diffie-Hellman paper. The three researchers published their finding in the MIT/Laboratory for Computer Sciences Technical Memo Number 82: "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," dated April 4, 1977.[86]

Martin Gardner, who wrote the "Mathematical Recreations" column for *Scientific American,* received a copy of the Rivest paper, and published a column on it in August 1977. They offered a challenge to readers: Rivest would generate a 129-digit public key and encrypt a message with it. Anyone who could decode the message without the private key – which meant breaking the key through factoring or a brute force attack (which Rivest erroneously estimated would take a quadrillion years on a very fast supercomputer, or at least a good long time) – would receive a $100 prize, and the RSA system would be

[85] Quoted in Levy, *Crypto* 89.

[86] Ron Rivest, Adi Shamir, and Len Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," MIT/ Laboratory for Computer Sciences Technical Memo, No. 82, April 4, 1977.

dumped. Readers were invited to try their hand at cracking the system, or at least to send an SASE to MIT to request a copy of the technical paper. This article was the first public (or at least beyond the world of *IEEE*) notice of the revolution in cryptography that had begun with the Diffie-Hellman paper. NSA was duly horrified, and its efforts to further restrict cryptography began in earnest.

For the first 25 years of its existence, NSA's relationship with Congress was smooth. Its contact was limited to a few representatives on classified intelligence committees, and the NSA's requests were routinely rubber-stamped. Because of the perceived monopoly and expertise of the NSA – an image the NSA tried very hard to encourage and maintain – and the highly technical nature of the topics being discussed, Congressmen tended to defer to the NSA on issues that were framed in terms of national security and intelligence gathering. Congressmen, particularly those in the committees that supervised the NSA, usually took NSA's contentions at face value, and usually did not question the NSA's motives. In part, this was because NSA's underlying ideology, with its emphasis on national security (which was highly dependent on SIGINT) as a primary interest, was in accord with the values of Congress during the Cold War. In addition, NSA had become very good at converting Congressmen to its cause:

> *NSA [Congressional] briefings were notorious in Congress. They involved a dramatic presentation by the NSA on why our international eavesdropping abilities were so vital, typically including a litany of victories achieved by clandestine snooping (victories that would have been unthinkable without billions of dollars in funding), and perilous international situations that required continued vigilance and support. Perfected by Bobby Ray Inman in his days as NSA director, they initiated legislators into the society of Top Secret, implicitly shifting their alliance from the citizenry to the intelligence agencies. A newly cleared congressperson would get a presumably unvarnished and reportedly terrifying dose of global reality, after which he or she thereafter could be assumed to dutifully support any demands of the National Security Agency, lest the Huns gain a purchase on our liberty. Representatives and senators had been known to venture into the bug-swept room and emerge grim faced, stunning their go-go staffers by remarking, "Well, maybe we should reconsider."*[87]

In short, it was a textbook case of regulatory capture, made possible by a very persuasive argument put forth by the NSA. The very Congressmen who were supposed to be keeping an eye on the NSA were in effect taking direction from them. By 1975-6, however, the system had begun to break down. The Senate Intelligence Committee, in part fueled by the public criticisms of NSA's role in crippling DES with a weak key, initiated an investigation of the NSA's activities, including an effort called Project Shamrock that included surveillance of American citizens without warrants. The final report of the investigation emphasized the threat to privacy the NSA's snooping activities constituted. It was, despite avoiding serious repercussions, probably a good time for the NSA to lie low.[88] Unfortunately, the timing of the RSA paper and Gardner's article were poor for the NSA. The promise of RSA was that universal private communications were indeed possible, exactly what the NSA feared. Its efforts to prevent this from

[87] Levy, *Crypto* 264.

[88] See Bamford, *Puzzle Palace*, and Levy, *Crypto* 106.

happening therefore continued. Each time, as predicted by bureaucratic politics theories, it was a perceived crisis in the public arena, usually in the form of public criticisms by academics, independent cryptographers, industry and/ or civil libertarians that would spark Congressional investigation and force the NSA to back down.

*Turf Wars: NSF Round 1*

The NSA's first efforts were, not surprisingly, targeted at the major source of cryptographic research outside of the Triple Fence: academia. Specifically, the NSA put pressure on the National Science Foundation (NSF), an independent government agency tasked with fostering research into all sorts of scientific endeavors, including mathematics and computer science. In June 1975, the NSA warned Fred Weingarten, the NSF official in charge of math and computer science grants, that NSA was the only government agency with the authority to fund research in cryptography. Understandably concerned that he was breaking the law, Weingarten held off on new grants until he could research the matter – only to discover that neither NSF lawyers nor the NSA could find any legal documentation to back up their claim. In 1977, despite still having no documentation or legal justification for their claims, the NSA sent their assistant deputy director for communications, Cecil Corry, to Weingarten again, again invoking a mysterious presidential directive granting the NSA sole control over cryptographic research. The NSF again reminded the NSA that no evidence of such a directive had been found. Weingarten did agree to forward relevant proposals to the NSA for technical review (to be used in evaluating the grant), but insisted the process be open. Corry then attempted to co-opt control in this bureaucratic turf war by sending a memo to Weingarten's boss, John Pasta, thanking him for agreeing to consider "security implications" in evaluating proposals. Pasta replied with a denial that any such promises had been made, and that NSF had not and would not make any such promises. As Weingarten recalled:

> "NSA is in a bureaucratic bind. In the past the only communications with heavy security demands were military and diplomatic. Now, with the marriage of computer applications with telecommunications… the need for highly secure digital processing has hit the civilian sector. NSA is worried, of course, that public domain security research will compromise some of their work. However, even further, they seem to want to maintain their control and corner a bureaucratic expertise in this field…"[89]

Indeed, it seems that in attempting to push the NSF out of the cryptographic sponsorship game, NSA was attempting to simultaneously defend (or rather, expand, since its technically did not have authority over

[89] See account in USHOR. Committee of Government Operations, Government Information, and Individual Rights Subcommittee, *The Government's Classification of Private Ideas,* 96th Congress, 2nd Session, 1980. See also Bamford, Diffie, Landau and Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," *Science,* Vol. 97, July 29, 1977, 438-40, all in Levy, *Crypto* 106-8; Fred Weingarten, "Cryptography: Who Holds the Key?" *SIAM News,* January/February 1997, 2; David Burnham, *The Rise of the Computer State* (Random House: New York, 1980), 139-40.

all cryptographic research in the civilian sector) its bureaucratic turf, its advantage in cryptographic knowledge, and its own organizational capabilities (in the form of its ability to easily and effectively perform its mission of reading SIGINT). Therefore, further attempts by the NSA to suppress cryptographic research continued.

*The Meyer Letter*

On July 7, 1977, a letter from an NSA employee named John Meyer arrived in the IEEE offices, stating that IEEE's recent publications on encryption and cryptology, and its sponsorship of symposia and conferences on the topic, including ones in foreign countries, may have violated the International Traffic in Arms Regulation code (ITAR). The letter included cites of specific subsections of various codes, and copies of the pages of the laws. ITAR, designed to "control the import and export of defense articles and defense services," classified "privacy devices [and] cryptographic devices" as "instruments of war", including not only the actual devices but any "technical data," defined as "any unclassified information that can be used... in the design, production... or operation" of these "weapons".[90] The problem was that Marty Hellman had already presented his ideas on public key at a conference – in Sweden. The letter also noted that a planned IEEE conference in Ithaca, New York that included papers on encryption could present a problem if preprints of papers were sent to international participants, as according to ITAR, an export license was required, a requirement that had been ignored at the Ronneby, Sweden conference. Naturally, as word of the letter leaked out, it caused some consternation among the conference participants: if Meyer was right, the speakers would be subject to jail time just for presenting their research.

The letter did not identify Meyer as an NSA employee, but he was outed by investigators at *Science* magazine. Although the NSA denied it any involvement in the letter, it aroused deep suspicions as to NSA's intentions to restrict independent cryptographic research. Later investigations were to show that Meyer had no instructions from the NSA to send the letter, as the NSA claimed, though the NSA refused to repudiate the letter, as it mostly represented what NSA thought, if not what it was willing to say publicly. The new NSA director, Adm. Bobby Inman, had begun what was functionally a war against cryptography outside of the Triple Fence.

The IEEE sent out a letter to six universities notifying them of the contents of the letter and the possible violation of ITAR regulations, noting that while IEEE was exempt from the regulations, the individual researchers were not. It suggested that they should send their papers to the Office of Munitions Control, Department of State, Washington, D.C. Unfortunately, sending publications to the State Department for review would effectively yield control of the work to the government, giving them the

[90] Text of ITAR regulations, quoted in Levy, *Crypto* 113.

opportunity, and, since the reviews were done by the NSA, to the NSA – with all of its interests in preventing the development and spread of crypto.

The researchers, back by their respective universities, did not cave, and indeed went public to the *Washington Post* and *New York Times* with the Meyer letter and their complaints, drawing down public criticism of the NSA. They did not believe that intellectual freedom should be compromised on the basis of undocumented, unproven claims of national security. Rivest checked in with the MIT administration, which ordered him to hold off sending out copies of the technical memo while it cleared the way for distribution of the memo. At Stanford, Marty Hellman, also scheduled to speak at the Ithaca conference, consulted university lawyers, who concluded that presenting his research was "not unlawful." The university counsel, however, also pointed out that in case he was wrong, while he would be happy to defend him, Hellman would be still be subject to fines or jail time if the government won.[91]

Still, despite all of these threats and dangers, the conference went on as planned. The professors did not vet their papers with the government and nothing happened. The MIT professors found a clause in ITAR regulations that provided an exemption on "published materials," and faced with NSA's inability to come up with a legal rationale for preventing distribution of the Technical Memo, MIT allowed its professors to proceed. In December 1977, the requested copies of the memo were mailed out, and the RSA algorithm went global.[92]

*Advances and Retreats: Secrecy Orders and more*

The NSA's efforts to suppress outside research proceeded despite its continuing inability to find legal documentation to back up its claims to authority over all cryptographic research. On April 28, 1978, the NSA slapped a secrecy order on a patent application for a device to produce stream ciphers using mathematical means submitted by a University of Wisconsin electrical engineering professor named George Davida. Although Davida had produced the plans without access to classified information and his funding from the NSF had no conditions attached requiring vetting with any defense agencies, the NSA declared his invention classified material anyway. This meant that not only could he not produce the device, he was forbidden from even discussing the ideas behind it. Unfortunately, as is typical in an academic environment, his ideas had already been well circulated, which meant he was required to report everyone who might have seen his work, including all of his colleagues. If he failed to do so, he was subject to a $10,000 fine and 2 years' imprisonment. The same day, the NSA also imposed a similar secrecy order on an invention called the "Phasorphone," a voice-scrambling device invented by a team of

[91] Levy, *Crypto* 113.
[92] *Ibid.* 114.

scientists lead by a technician named Carl Nicolai. Nicolai had hoped to make a fortune off his device; instead, he was now forbidden from even admitting its existence.

Both Davida and Nicoli fought the order. They took their cases public, going to the media, organizing letter-writing campaigns, informing their congressmen. University of Wisconsin officials met and sent a letter to the NSF, demanding due process. The chancellor also took the case to the Secretary of Commerce, Juanita Kreps, who had been unaware of the case and was incensed to find her patent office being used for censorship purposes. The NSA backed down in the face of the firestorm, rescinding the Davida order a little over a month later with the excuse that it had been a mistake by a mid-level employee. A few months later, the secrecy order on the Nicolai patent was also lifted. The Director, Bobby Inman, could not blame that mistake on a mid-level employee, as he had signed the order himself. Instead, he claimed a "heat of battle" excuse to the House subcommittee investigating the issue.[93] Thus again, as with the Congressional investigations in 1975, it took a perceived to force other branches of the government to act, and force the NSA to back down.

*Turf Wars II: NSF, Round 2*

By late 1977, Admiral Bobby Inman, who had taken over only the directorship of the NSA a few months ago in July, decided enough damage had been done to the Agency's reputation and that a public appeal was necessary. He began a tour of various research institutions to diffuse the anger and growing perception that the NSA was trying to restrict cryptographic research, whether by actively impounding it or by luring researchers under NSA's jurisdiction, where their findings could be classified. His university tour was not successful, though it did illustrate the NSA's growing recognition of and adaptation to the changes in the cryptographic world outside. It did not, however, illustrate a shift in the NSA's ultimate goals.

Len Adleman, the "A" of RSA, discovered this when he tried to renew his long-running NSF grants on his mathematics research. In a section of his grant proposal, he had mentioned some new work that might apply to cryptography. He was soon informed by NSF officials that the portion of his research that applied to cryptography would be funded by the NSA, which would subject it to review (and potential classification and impoundment) by the NSA under the grant's conditions. Adleman objected, stating that he had submitted his proposal to the NSF, not the NSA. As it turns out, NSA had put pressure on the NSF yet again, in yet another attempt to assert control over all cryptographic research in the

[93] Levy, *Crypto* 116-7. For notes on Davida case, see Deborah Shapley, "DOD Vacillates on Wisconsin Cryptography Work," *Science*, Vol. 201, July 14, 1978, 141; Louis Kruh, "Cryptology and the Law–VII," *Cryptologia*, Vol. 10, No. 4, October 1986, 248; Bamford, *Puzzle Palace*, 449-50. For notes on Nicolai case, see Deborah Shapley, "NSA Slaps Secrecy Order on Inventors' Communications Patent," *Science*, Vol. 201, September 8, 1978, 891-94; Kruh; Bamford, *Puzzle Palace* 446-51.

country. Adleman, while recognizing the possible national security implications of cryptographic research, believed the NSA was overstepping its bounds in attempting to influence academic research through the NSF. "In my mind this threatened the whole mission of a university, and its place in society," he stated.[94] Adleman went public, to Gina Kolata of *Science* magazine, who had been covering the conflict since the Meyer letter days. Soon afterward, Adleman received a call from Bobby Inman, saying the whole matter was "a misunderstanding." It seems, from the Davida-Nicolai-Adleman experiences, that the only thing that could rein in the NSA was a public outcry, or in the terminology of organization theory, a "crisis" in the form of the threat the NSA posed to the freedom of academic research.

*The First Amendments and other costs*

Despite these public setbacks, Inman still believed that the NSA had the upper hand because of ITAR regulations. He believed that the key to control of cryptography was export laws, and that they were the only thing that prevented a "disastrous free-for-all in the distribution of cryptography—the equivalent of a national security meltdown."[95] The export controls and threat of prosecution would force people to deal with NSA, and because products for export were linked to those for domestic use, the NSA could effectively by extension also control domestic encryption as well. This was the way around NSA's lack of formal legal authority to control encryption in the U.S., the very problem that the NSA had run into in its turf wars with the NSF. Thus, "those regulations would become the linchpin of the agency's efforts to stop worldwide communications from becoming ciphertext."[96] The issue of the DES algorithm, and now the RSA algorithm, being already widely distributed around the world, and all the implications of that distribution for the effectiveness of export controls as a way of limiting cryptography does not seem to have sunk in. Moreover, Inman's faith in the power of the ITAR regulations was soon to be undermined. Prompted by the recent public controversies over encryption, the White House Science Advisor, Frank Press, had asked the Justice Department to look into the legality of ITAR regulations with respect to the First Amendment's protections for free speech. The opinion of the Office of the General Counsel, issued May 8, 1978, declared that:

> *It is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector.*[97]

[94] Levy, *Crypto* 118, presumably from interview.
[95] *Ibid.* 119.
[96] *Ibid.* 119.
[97] John M. Harmon, "Constitutionality Under the First Amendment of ITAR Restrictions of Public Cryptography," memo to Dr. Frank Press, science advisor to the President, May 11, 1978. Reprinted in Hoffman, *Building in Big Brother.*

However, the Justice Department, by not circulating its opinion, in effect rendered its own findings moot – and the NSA blithely ignored the implications of that opinion, continuing to interpret export laws to suit its purposes. Clearly, as far as the NSA was concerned, its organizational interests and national security still far outweighed any other values at stake. The story itself did not come out until 1980, when the government operations subcommittee of the House held hearings on "The Government's Classification of Private Ideas." Tim Ingram, the committee staff director, pointedly asked the Justice Department:

> *You have this two-year-old opinion finding the regulation unconstitutional. There has been no change in the regulation. Is there any obligation on the department at some point to go to the President and force the issue and to tell the President that one of his executive agencies in currently in violation of the Constitution?*[98]

The ITAR exemption for "technical publications" that had freed IEEE from worries of prosecution during the Meyer letter days was rewritten "to make it clear that the export of technical data does not purport to interfere with the First Amendment rights of individuals," thus closing another loophole for the NSA and forcing them to adapt their strategy yet again.[99]

*NSA Goes Public*

Meanwhile, Bobby Inman at the NSA fretted over the new developments in cryptography and his limited ability to stop it. He feared that public adoption of encryption "would very directly impact on the ability of the NSA to deliver critical information" – an admittedly valid fear. In attempt to secure formal authority over cryptography, perhaps in reaction to the success academics had had in fighting the NSA itself in the press, Inman went public. This was quite a departure from the norm for an agency whose existence only years ago was not even acknowledged. He published an interview in *Science,* the publication that had been most vigilant in reporting on the cryptography debate in the past few years. Inman proposed a dialogue between the academic community and the NSA to find a middle ground between academic freedom and classified research. He acknowledged, however, that a debate was more likely than a discussion. Inman also delivered a public speech (granted, to a group of defense contractors) in defense of his agency in January 1979, attempting to convince listeners – and by extension, the public – that it was necessary to do things his way. He denied accusations that the NSA had influenced the specifications of DES (probably not true), used export controls to regulate scholarly work (definitely not true), or attempted to curtail research grants on cryptography (also not true). If anything, he argued that while the public saw the NSA as an all-powerful agency, its real problem was that it had too little. As far as Inman was concerned, the lack of actual laws granting it a legal monopoly over cryptographic research was simply an oversight, a holdover from the days when the technical barriers alone kept outsiders from

[98] Levy, *Crypto* 119.
[99] See text of ITAR at http://pmdtc.org/reference.htm.

investigating cryptography, and it was one that should be corrected. National security was being sacrificed at the altar of civil liberties and free speech, and NSA, which only sought to protect national security, was being unfairly demonized in the press.[100]

Eventually, a compromise of sorts was reached. An American Council on Education study panel was set up, and it recommended a two year experiment in which cryptography researchers could voluntarily submit papers for pre-publication review. The NSA could warn the researcher if it decided the information would compromise national security but could not impound the paper and prevent its publication. Both the NSA and NSF would continue to fund research, but taking NSA funds (with their attendant restrictions) would be optional. George Davida, whose invention had been subjected to secrecy order that was later withdrawn, issued a minority report for the panel, dismissing NSA concerns that cryptography research would help enemies' cryptanalysis attempts, because the research in question was on cryptography, not cryptanalysis. He concluded that, "the NSA's effort to control cryptography [is] unnecessary, divisive, wasteful, and chilling. The NSA can perform its mission [the cryptanalysis aspect of its mission, not the cryptography aspect] the old-fashioned way: STAY AHEAD OF OTHERS [caps in original]."[101] This dissent, perhaps colored by Davida's own experience with NSA censorship, was disingenuous. In fact, yearly Crypto conferences, meetings of cryptographers from around the world, began a year later, and the second conference, Crypto '82, featured a panel on cryptanalysis.[102] Still, the system worked well. The NSA did not attempt to overstep its bounds, occasionally submitted comments to the authors, and went no further. The NSA even helped push through publication of an article that the Army had tried to silence. Of course, the NSA had not done so out of altruism, but to preserve its pre-publication review privileges, which was generally successful due to high rates of.[103]

This amicable relationship ground to a halt in 1989, when the NSA attempted to suppress a paper written by Ralph Merkle, which according to the terms of the prepublication review it had agreed not to

[100] Text of Inman's speech is reprinted as "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector" in Bruce Schneier and David Banisar, eds. *The Electronic Privacy Paper* (New York: J. Wiley, 1997), 347.

[101] Dissent reprinted in Davida, "The Case Against Restraints on Non-governmental Research in Cryptography," reprinted in *Cryptologia,* Vol. 5, No. 3, July 1981, 143.

[102] Shamir and Adleman, of RSA, were both scheduled to speak, and Adleman publicly tested a cryptanalysis scheme on his Apple II personal computer against a popular variant of public key cryptography, Ralph Merkle's knapsack scheme. Having been challenged to break the knapsack scheme on the first day of the conference, Adleman had programmed his computer to break through a knapsack encryption. While Adleman spoke, discussing different techniques for attacking different knapsack systems with different characteristics, Carl Nicolai (the one whose Phasorphone had been impounded by the government a few years earlier), used the Apple II to break the knapsack. At the end of the talk, the knapsack was broken. See Levy, *Crypto* 128 for discussion.

[103] Susan Landau, "Zero Knowledge and the Department of the Defense," *Notices of the American Mathematical Society (Special Article Series),* Vol. 35, No. 1, 1988, 12, cited in Diffie and Landau 254.

do. [104]Merkle, now working at Xerox's Palo Alto Research Center, had written a paper that introduced a series of algorithms that would speed up cryptographic communications and drive down the price of encryption, as well as discussing the technology of S-box design – a sensitive topic since the Lucifer days. Xerox, a government contractor, had submitted the paper in the hopes of one day getting an export license for products based on Merkle's work. As a government contract with future contracts to lose, Xerox agreed to suppress the paper. However, one of the outside reviewers was so upset at the suppression that it leaked the paper to an independent watchdog, a computer-hacker millionaire named John Gilmore, who promptly posted the paper up on the Internet. In fact, he posted it to the Internet discussion group sci.crypt, a sort of 24-hour virtual gathering space for cryptographers around the world, so within minutes, the paper was on 8000 computers around the world, and the NSA's prepublication system became irrelevant.[105]

*Lotus Notes and the commercialization of cryptography*

Turning to the commercial sector, the early 1980s also marked the beginning of commercial mass market cryptography. In 1983, after failed attempts to put the RSA algorithm on a chip, the three RSA inventors decided to incorporate, forming RSA Data Security, Inc.[106] They obtained a license for the RSA algorithm from MIT, which held the patent, and produced a commercial software program called Mailsafe to encrypt e-mail and store data on IBM PCs and clones. Eventually, they joined with Iris, a small software company owned by Lotus, which was developing Notes, a groupware program (a program shared by dozens or thousands of people over a networks) that was a natural candidate for encryption system because it assumed all users would communicate electronically. The problem, however, came in the market of Notes. Because overseas customers would constitute over half of projected sales, Notes, which had built-in RSA encryption, was subject to federal export controls. (The export controls were not a problem for RSA, which shipped Mailsafe only within the U.S.).

Lotus soon found itself mired in a tangle of export regulations. Never before had anyone tried to sell a mass market program that included encryption, and Notes used RSA for the key exchange and DES for the actual encryption, two technologies that by this time were highly out of favor with the NSA. The use of both in mass market commercial software was the NSA's worst nightmare, as it had all the features the NSA hoped to avoid: easy-to-use, built-in, strong encryption. It circumvented almost all of the reasons why encryption was not widely used: ease of use (since cryptography was generally not user-friendly and

[104] Ralph Merkle was the inventor the knapsack scheme, one of the first attempts to implement a workable public key cryptography scheme, and remains a pioneer in public key cryptography. His knapsack scheme was broken at a cryptography conference by Len Adleman.
[105] John Markoff, "Paper on Codes is Sent Despite U.S. Objections," *NYT,* August 9, 1989, in Levy, *Crypto* 166-7.
[106] Chip manufacturing technology simply wasn't up to putting such complicated algorithms on so small a space yet.

remained largely the domain of large organizations and computer geeks), ready availability (since most individual users were not even aware of the need for cryptography, they were unlikely to seek it out), and strength. Export licenses for cryptography were generally only issued with end user certification, usually to a company with ties to the military establishment or to large financial institutions (financial clearinghouses, banks). It was mid-1986 by the time Ray Ozzie, the inventor of Notes, went down to Fort Meade to meet with the NSA about the export regulations, an effort that almost immediately stalemated.

As only selling within the U.S. meant giving up over half of potential revenues, it was not an option for a company dependent upon economies of scale for profitability. The NSA, however, played hardball, threatening to stop shipments of Lotus' number one money-making program (and the most popular software program in the world), the Lotus 1-2-3 spreadsheet, which made most of its sales overseas, on the grounds that it contained encryption. Actually, what it contained was a password access feature. While it was unlikely that the U.S. government would actually stop shipments of software that only used passwords, the willingness of the NSA to make the threat shows its desperation to exert control over encryption – at any cost.[107]

Eventually, a compromise emerged. Lotus would drop DES as the encryption algorithm and use a new cipher, which the NSA would evaluate and approve for export, with a key length to be negotiated later. Lotus eventually settled on RC-2, a new cipher written by Ron Rivest, with a variable key length. Negotiations continued for another two years, until 1989 when Notes was finally ready to ship, but there seemed to be no export solution in sight. Ozzie was convinced that there was a factional struggle going on within NSA over how to proceed.[108] In mid-1989, the NSA (verbally) proposed a compromise: 32-bit keys for export, a number that allowed for a keyspace of about 4 billion keys – a figure that NSA representatives admitted they could crack in a few days (and probably sooner). It was a weak enough key that even linking together a few dozen personal computers could crack the key within two months, and per Moore's law, much sooner as technology improved. Lotus could not get NSA to budge, so eventually, two versions were produced: a 32-bit international version, and a 64-bit domestic version. In order to ensure interoperability, the domestic version had to be programmed with two sets of keys, one for use communicating with other domestic customers, and the other with international customers, a programming nightmare that complicated production and added to the cost of the program, just as production of two versions did. The international backlash – the questions of 'why do we have a weaker

[107] See Levy, *Crypto* 159 for discussion of NSA threats to Lotus 1-2-3.

[108] *Ibid.* 160. Unfortunately, I cannot find any documentation of this, though it seems an entirely plausible explanation. It would fit in with the pattern of behavior found during the DES approval process, when the NSA was forced to balance COMSEC demands (creating a strong cipher for government use) with COMINT considerations (preventing anyone from understanding how the NSA made ciphers).

version? – did not begin until a few years later, when the novelty of having a mass-market program with built-in encryption began to wear off.

NSA thereby forced the production of *two* versions of Notes, one with strong 64-bit encryption for domestic use (which NSA couldn't regulate under the Computer Security Act), and one with reduced 40-bit encryption for export. Lotus, on the other hand, considered 40-bit keys a compromise to get the product out the door, with the idea that once its customers got a taste for encryption (hopefully customers with influence on the government), they would help Lotus fight for stronger encryption and longer key lengths.[109] The NSA, meanwhile, was pulling in the opposite direction, suggesting changes in the key design that would prevent re-encryption (encryption of already encrypted messages), which would make deciphering messages more difficult, but which made the program run more slowly. A few years later, faced with a similar problem, Microsoft would for ease of manufacturing choose to only distribute a single, weak (40-bit) version of its products, which Ray Ozzie called "espionage enabled encryption".[110] Hence we see the price industry paid for NSA's quest to ease its own work: creation of two versions of software; complications in programming to coordinate the two versions; potential loss of sales and/or reputation due to international backlash against 'discriminatory', second-class products; and diminished quality of product. Consumers, meanwhile, paid for it in the form of increased costs (increased manufacturing costs passed on to consumers), and less security and privacy.[111]

[109] *Ibid.* 163-4.

[110] *Ibid.* 262.

[111] A few years later, in 1990, NSA would try to strong-arm the new corporate giant in software, Microsoft, fueled by an increased sense of urgency in keeping strong cryptography out of commercial software – and, perhaps, eliminating rivals to its own proposed standard. RSA was on its way to signing a deal with Microsoft to put the RSA algorithm into Windows, the ubiquitous operating system. The NSA probably recognized that once Microsoft, which controlled a vast majority of the personal computing market, adopted RSA it would be difficult to enforce its own standard. According to Nathan Myhrvold, Microsoft's Chief Technical Officer at the time, the NSA tried to turn him against Jim Bidzos, RSA's President, and RSA during discussions of export licenses. The agency representatives dropped hints that the RSA cipher had been cracked by analysts at NSA, which understandably worried Myhrvold, since the reputation of his company depended on putting in reasonably strong security. Bidzos promptly fought back by contacting every mathematician, number theorist, cryptographer and researcher that RSA could find, within a day could refute the insinuation. The charge boiled down in essence to the ongoing debate over the relative security of private versus public algorithms, with the idea being that public algorithms, because they have been tested by challenges by anyone in the cryptographic community, could be trusted more than NSA's secret algorithms. As Bidzos pointed out, RSA had a strong incentive to make sure its algorithm was strong: once the algorithm was broken, the company had no value. Luckily for RSA, Myhrvold was convinced, and took the NSA's objections as a reverse-psychology endorsement: why else would they object, unless the algorithm really was strong? Myhrvold also recounted a last-minute attempt by the agency to discourage Microsoft from licensing RSA, questioning the (admittedly complex) validity of the RSA patents and suggesting that since future government standards would not use RSA, Microsoft would be stuck with a set of algorithms that were not interoperable with the government standard (and by extension, the most commonly used algorithms). A final attempt boiled down to an agency official calling Myhrvold and saying, in essence, "Don't do it," and that it would be a mistake to license RSA. Microsoft signed with RSA anyway. See Levy, *Crypto* 175-6, for account of Microsoft-NSA episode.

*CCEP and the Poindexter Directive*

By the mid-1980s, NSA had learned to regret its original decision not to submit an algorithm in response to NBS's 1973 request for an encryption standard. DES had become unexpectedly popular, and far as the NSA was concerned, it was time to replace it with something more acceptable to NSA's interests. Aided by the development of tamper-resistant coatings for chips, NSA now attempted to create a Commercial COMSEC Endorsement Program (CCEP) that would supplant the DES and replace it with a new NSA-designed cryptosystem, dubbed "Project Overtake."[112] NSA's rationale was that widespread use of DES could prompt a hostile intelligence organization to mount an attack on the cipher, which ironically had been weakened earlier by NSA's insistence on cutting the key length.[113] This, however, was probably disingenuous; the real problem was that DES was too strong, so that widespread use of DES, especially if inserted in mass market, user-friendly programs like Notes would increase the difficult of monitoring communications exponentially. Thus the NSA needed to nip the problem in the bud, preferably by replacing it with its own cipher, which would be under its control.

NSA intended for CCEP to secure a wider range of American communications, including industrial communications. It also intended for it to be done with industry money, as the program was open to companies with SECRET facility clearances willing to contribute expertise and funding to the development of secure versions of their products. The initiative split equipment into two categories: Type I (with administrative controls applicable to protection of classified info), and Type II (protection of unclassified sensitive info, without administrative controls). NSA's idea was Type II would compete directly with DES and eventually replace it. However, industry didn't bite. The equipment was bulky and expensive, costing over $1000 per computer to implement. The banks and other financial institutions being asked – or rather, ordered, according to one banking executive's account of a typical NSA sales call – to participate were given no control over the system: neither the algorithms (provided by the NSA), nor the equipment (tamperproof), nor even the keys (generated and distributed by the NSA itself). In response to criticisms that the NSA might be keeping copies of those keys for itself to ease its decryption, the NSA spokesman's response was "We have better things to do with our time."[114] The banking community and their DES suppliers, not surprisingly, rejected the NSA's demands, especially since it had only been a few years since they had been forced to spend large amounts of money on government-certified DES. Moreover, banking, as an international industry, had negotiated special export arrangements that allowed it to operate and coordinate communications using the same cryptosystems. A secret, NSA-designed,

[112] Ellen Raber and Michael O. Riley, "Protective Coatings for Secure Integrated Circuits," *Energy and Technology Review,* May-June 1989, pp. 13-20, in Diffie and Landau 64.

[113] Bob Davis, "A Supersecret Agency Finds Selling Secrecy to Others Isn't Easy," *Wall Street Journal,* March 28, 1988.

[114] *Ibid.*

American-access-only cryptosystem was hardly designed to inspire confidence in foreign partners, and the necessity of communications with them made adopting the same system essential.[115]

In the end, despite NSA's gambit, NBS recertified DES over NSA's objections. NSA, in turn, reneged on its original promise to not restrict Type II equipment, and citing the Computer Security Act of 1987, imposed controls almost as strict on Type II equipment as well.[116]

The next salvo in the war between the NSA and civilian cryptographers came in the form of National Security Decision Directive (NSDD-145), issued by President Ronald Reagan in September 1984. It established federal policy of safeguarding "sensitive but unclassified" information in communications and computer systems, a policy heavily influenced by the NSA.[117] The Poindexter Directive, named for the President's National Security Advisor, attracted a lot of attention and eventually Congressional scrutiny. All federal executive branch departments, agencies, and their contractors, *including civilian companies not doing secret work* (e.g., the Lexis-Nexis supplier, Mead Data Central), were affected. Teams of government representatives, including people from the NSA, FBI, CIA, and the U.S. Government Intelligence Committee, began to visit these various agencies and contractors. The FBI visited university libraries, demanding information on which materials foreign students were accessing, a demand refused by university librarians who demanded subpoenas in exchange.[118] A House of Representatives investigation ensued, and a turf battles between Congress, which saw the directive as an incursion of presidential authority into national policy, and the Presidency began. The Poindexter Directive was withdrawn soon after Congressional hearings began.[119]

[115] Cheryl Helsing, Chair, Data Security Committee, American Bankers Association, and VP for Corporate Preparedness and Information Security, Bank of America, Testimony in USHR 100a, 113-114 (1987), in Diffie and Landau 67.

[116] From Diffie and Landau 64 and footnotes: Type I equipment is managed through COMSEC accounts, which are basically only available to organizations with government contracts. Users of Type II equipment would not have COMSEC accounts (this would have included the banking industry), but would need to obtain equipment from government sponsors. From a functional standpoint, the difference was minor.

[117] Clinton C. Brooks, Memo, April 28, 1992, in Banisar, *Electronic Privacy Papers,* 1996.

[118] Interestingly, a practice now permitted by the Patriot Act.

[119] This may have had something to do with the political conditions of the time. The Reagan administration was then in the middle of the Iran Contra hearings, and feared that putting Poindexter in front of a Congressional committee would inevitably lead to questions on the Iran Contra affair. Poindexter in fact did not appear until subpoenaed (United States House of Representatives, Committee on Government Operations, Subcommittee, *Computer Security Act of 1987,* Hearings on HR 145, February 25, 26, and March 17, 1987, 100th Cong., 1st Sess., 1987, 381), and after a delay of two weeks of negotiations between the White House and the committee, he pleaded the Fifth when he did take the stand, despite being promised that questions would be limited only to the Directive. In the interim, the administration withdrew the directive, hoping to avoid Poindexter's appearance in Congress. The committee, having achieved the withdrawal of the Directive, did not pursue the matter. This is in the notes to pg. 68 in Diffie and Landau, and references Frank Carlucci, Letter to Chairman Jack Brooks, March 12, 1987, in USHR 100a, 386 (1987).

*Turf Wars III: Computer Security Act of 1987*

The hearings over NSDD-145 resulted in yet another piece of legislation, the Computer Security Act (CSA) of 1987.[120] Congress wanted to re-establish and clarify who was in charge of assessing the security of civilian computer systems. NSA lobbied for the role, arguing that it had the largest collection of staff dedicated to computer security in the U.S., and that creation of a second organization would create a redundant bureaucracy.[121] Congress, still fresh from the fight over the NSA-influenced Poindexter Directive, disagreed. It gave the job to the NBS (later renamed the National Institute of Standards and Technology, or NIST), putting them in charge of developing computer security standards for the civilian sector on the grounds that developing security standards for civilian use was different from doing so for government use, and that the NIST had 22 years' of experience doing so while the NSA had none.[122] In doing so, the House Government Operations Committee pointedly noted that: "NSA has made numerous efforts to either stop [work in cryptography] or to make sure it has control over the work by funding it, pre-publication reviews or other methods."[123] According to the legislation, the NSA's only role was to *consult* with NIST, as the House committee was explicit that NIST was to be in charge. The committee recognized that "By putting NSA in charge of developing technical security guidelines... [NIST], in effect, would on the surface be given the responsibility for the computer standards program with little say about most of the program – the technical standards developed by NSA. This would jeopardize the entire Federal Standards program."[124]

A TOP SECRET memo from Clinton Brooks, the Special Assistant to the Director of the NSA, summarized the Agency's evaluation of the situation: they'd been out-maneuvered. The text of the memo:

- *In 1982 NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all U.S. information systems to the Director of NSA, eliminating NBS from this.*
- *This also stated that we would assist the private sector. This was viewed as Big Brother stepping in and generated an adverse reaction.*
- *Representative Jack Brooks, chairman of the House Government Operations Committee, personally set out to pass a law to reassert NBS's responsibility for Federal unclassified systems and to assist the private sector.*
- *By the time we fully recognized the implications of Brooks' bill, he had orchestrated it for a unanimous consent voice vote passage.*

*Clinton Brooks*
*Special Assistant to the Director of the NSA*
*April 28, 1992*[125]

[120] Public Law 100-235.
[121] William Odom, Testimony in USHR 100a, 294-5.
[122] United States House of Representatives, Committee on Government Operations, House Report 100-153, Part 2, *Report on the Computer Security Act of 1987*, 100th Cong., 1st Sess., Washington, D.C., in Diffie and Landau 68.
[123] *Ibid.* 21.
[124] *Ibid.* 26.
[125] Clinton C. Brooks, Memo, April 28, 1992, in Banisar, *Electronic Privacy Papers*, 1996.

Despite this setback, the NSA still had one last card to play, and it played it well. Although Congress had given the authority to NIST, NIST lacked NSA's resources as the largest employer of mathematicians in the U.S.. NSA's unclassified budget funded 300 employees at a cost of $40 million; NIST's computer security operation had 16 employees and only $1.1 million.[126] The Congressional Budget Office (CBO) estimated of the cost of implementation of the Computer Security Act ranged from $4-5 million per year.[127] As such, the NSA negotiated with the acting head of NIST, Raymond Kammer, to formalize an understanding of NSA and NIST's respective responsibilities in the development of cryptography. A Memorandum of Understanding (MOU) was drafted that mandated that NIST would "request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques."[128] A Technical Working Group (TWG) was set up, with three members each from the NSA and NIST, which would review and analyze issues of interest *prior to public disclosure.*[129] The prior review put NSA in a position to control development of civilian computing standards. Moreover, it circumvented the intent of the Computer Security Act, which gave authority to approve standards to the Secretary of Commerce. The MOU changed the implementation of the legislation so that appeals could also be routed through DOD to the Secretary of Defense before public airing in addition to – and instead of – the Commerce Secretary. Disagreements in the TWG could be routed through to Commerce or Defense, and from there to the president and the NSC, the source of NSDD-145. In short, the NSA executed a bureaucratic coup, expanding its bureaucratic turf to explicitly forbidden territory.

Observers were horrified at the blatant disregard for the letter and intent of the CSA. Milton Socolar, a special assistant to the Comptroller General of the GAO, testified before Congress: "At issue is the degree to which responsibilities vested in NIST under the [Computer Security] act are being subverted by the role assigned to NSA under the memorandum."[130] The Office of Technology Assessment (OTA) wrote that the MOU ceded "to NSA much more authority than the act itself had granted or envisioned, particularly through the joint NIST/ NSA Technical Working Group."[131] In fact, the only person outside

[126] United States Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, 164.
[127] USHR 100b, p. 43
[128] United States Department of Commerce, National Institute of Standards and Technology, and United States Department of Defense, National Security Agency, "Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency concerning the Implementation of Public Law 100-235," March 24, 1989, 2.
[129] *Ibid.* 3.
[130] Milton Socolar, Testimony of, in United States House of Representatives, Committee of Government Operations, Legislative and National Security Subcommittee, *Military and Civilian Control of Computer Security Issues,* Hearings on May 4, 1989, 101st Cong., 1st Sess., 1989, 36-49.
[131] USC-OTA 1987, 164.

of the NSA who didn't seem to agree with this evaluation was the head of NIST itself. (His staffers, however, were quite convinced that they'd been outmaneuvered.)

Further evidence of NSA's success in subverting the intent of the CSA and asserting control over cryptographic standards came in the form of the debate over the digital signature standard. As part of the Computer Security Act, the NIST was required to establish standards for various aspects of computing, including digital signatures, encryption, key exchange, etc. The first of these to come up was digital signatures, the technology that allows verification of the identity of the sender or source of a particular message. The legal implications of such a technology were fairly obvious; without it, electronic communications were subject to disputes over authenticity, making contracts and e-commerce impossible. TWG meetings to set up a public key based standards began in spring 1989. NIST proposed the RSA algorithm, which had not been successfully broken in twelve years despite multiple attempts.[132] The NSA rejected the proposal, and for more than a year, the discussion stagnated. As Lynn McNulty, NIST's Associate Director of Computer Security, stated, "We went to a lot of meetings with our NSA counterparts, and we were allowed to write a lot of memos, but we on the technical side of NIST felt we were being slowrolled on the Digital Signature Standard. In retrospect, it is clear that the real game plan that NSA had drawn up was the Capstone Chip and Fortezza card – with key escrow all locked up in silicon."[133]

In 1990, the NSA proposed its own standard, a secret algorithm developed by an employee of NSA, David Kravitz. Its justification was a classified TOP SECRET CODEWORD document that contained the arguments for selecting this particular algorithm.[134]

Industry objected to the algorithm on several grounds:

- it was not interoperable with existing digital signatures already in use
- the algorithm had been shown to be not particularly secure even with the proposed 512-bit key[135]
- for signature verification, it was roughly 10 times slower to use than RSA on comparable processors (though 25 times faster for the actual signing)[136]
- the key could be used for signing only, not encryption[137]

[132] United States General Accounting Office, *Communications Privacy: Federal Policy and Actions,* (Letter Report, April 8, 1997, GAO/AIMD-97-49), 20, in Diffie and Landau 72.

[133] Private conversation between Landau and McNulty, cited in Diffie and Landau 72.

[134] United States Department of Commerce, National Institute for Standards and Technology, "Memorandum for the Record, March 26, 1990," in Computer Professionals for Social Responsibility, David Banisar and Marc Rotenberg, eds. *1993 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls,* 1993.

[135] Brian LaMacchia and Adnrew Odlyzko, "Computation of Discrete Logarithms in Prime Fields," *Design, Codes, and Cryptography,* Vol. 1, 1991, pp. 47-62; Th. Beth, M. Frisch and G.J. Simmons, eds., *Public Key Cryptography: State of the Art and Future Directions,* Lecture Notes in Computer Science, No. 578, Springer-Verlag; cited in Diffie and Landau 73.

[136] United States Department of Commerce, National Institute of Standards and Technology. *Publication XX: Announcement and Specifications for a Digital Signature Standard (DSS),* August 19, 1991.

These characteristics, however, conformed nicely to NSA's organizational interests. The lack of interoperability meant that in order to do business with or even have dealings with the government, which was inevitable, companies and by extension individuals would be forced to adopt the standard.[138] The relative lack of security would keep the balance between NSA's COMSEC and COMINT branches, producing a cipher strong enough to be credible but easy enough to break if necessary. The inability to use the algorithm for encryption meant that the NSA would achieve its 'best-case scenario' for SIGINT: communication in the clear.

Given the circumstances, it should not be surprising that critics believed that NSA was behind the abandonment of RSA as NIST's proposed signature standard, charges denied by NIST director John Lyons.[139] A memo released through Freedom of Information Act litigation, however, shows that NIST members of the TWG disagreed: "It's increasingly evident that it is difficult, if not impossible, to reconcile the requirements of NSA, NIST and the general public using the approach [of a TWG]."[140] The NIST's internal oversight group, the Computer System Security and Privacy Advisory Board, wrote in March 1992 that "a national-level public review of the positive and negative implications of the widespread use of public and private key cryptography is required." NSA resistance, however, squelched the idea. "The National Security Agency has serious reservations about a public debate on cryptography," stated the new NSA director, Admiral Michael McConnell, in a classified internal memo.[141]

The Congressional hearings on the digital signature standard focused on the continued tension between the NSA and NIST, and on which should be in charge of the government's computer standards program.[142] The House Government Operations Committee report on the CSA stated simply that the "NSA is the wrong agency to be put in charge of this important program."[143] Outside observers, including the OTA and GAO, concluded the MOU had effectively undermined the CSA and put NSA back in charge. As the OTA report put it, "Observers—including OTA—consider that [the MOU] appears to cede to NSA much more authority than the act itself had granted or envisioned, especially considering the

[137] Levy, *Crypto* 178.

[138] Setting a federal standard does not in itself force industry to adopt it; it is the pressure generated by the government's own operations, a sort of critical mass for the network effect, that makes it a de facto civilian standard.

[139] John Lyons, Testimony in USHR, Committee on the Judiciary, Subcommittee on Economic and Commercial Law, *The Threat of Foreign Economic Espionage to U.S. Corporations,* Hearings on April 29 and May 7, 1992, 102nd Cong., 2nd Sess., 163-176.

[140] United States Department of Commerce, National Institute of Standards and Technology, "Memorandum for the Record, January 31, 1990," in CPSR 1993.

[141] Levy, *Crypto* 184.

[142] United States Department of Commerce, National Institute for Standards and Technology, "Memorandum for the Record, March 26, 1990," in CPSR 1993, 19.

[143] USHR 100b, 19.

House report accompanying the legislation."[144] GAO's evaluation stated: "NIST follows NSA's lead in developing certain cryptographic standards."[145] The DSS proposal was put forth officially in 1991. After modifying the algorithm to accept a flexible key size (512-1024 bits), the standard was finally adopted in May 1994, over the objections of industry and academia.

Buoyed by this victory, the NSA continued its efforts to undermine the CSA by recruiting allies with similar sympathies and ideologies against the civilian NIST. Although its attempts to include the FBI as an equal member of the TWG had failed after the NIST staffers objected, Kammer (acting director of NIST) and Clint Brooks (advisor to Director of NSA) continued to recruit the FBI as an ally. Initially, according to Brooks, the FBI didn't understand the issue.[146] After some effort, the NSA convinced the FBI that encryption was indeed an important and critical issue that threatened the FBI's treasured wiretapping, and Kammer and Brooks converted what would soon become a valuable ally. An interagency group was formed with both the NSA and NIST, but now the NIST – whose staffers seemed often to be at odds with their acting head Kammer – was outnumbered. The NSA, recognizing that the end of the Cold War weakened its arguments on national security in the public's eyes, sought out allies whose motives and justifications – law enforcement – would be palatable to the American public, and by extension to Congress.[147] By 1991, the FBI had come up with a policy to strengthen its electronic surveillance capabilities, especially wiretaps, and *to prevent the establishment of unbreakable cryptography in the public sector.* These included a wiretapping bill that would force telephone carriers to make wiretapping easier, and key escrow, a concept that would fundamentally alter the debate on civilian cryptography.

[144] USC-OTA 1994,13-14.

[145] US-GAO, "Communications Privacy: Federal Policy and Actions," GAO/OSI-92-2-3 (November 1993); Levy, *Crypto* 183.

[146] Private conversation between Landau and Kammer, January 17, 1997, in Diffie and Landau 75.

[147] Diffie and Landau 76.

## Chapter 3

The years 1991-99 marked a sea change in the environment for computing and cryptography. As electronic and digital communications became increasingly intertwined with daily life, the need for cryptography and public awareness of that need grew in tandem. The advent of online commerce and the increasing volume of financial transactions processed over phone lines and optical cables, too, fueled the push toward greater access toward cryptography. The growth of the Internet, perhaps, was most significant in this fight, in that the Internet provided not only a medium that fed the need for cryptography, but a way to access it (in the form of software downloads) and a means of organizing to get it (as with the Cypherpunk mailing list). The software industry, which had taken off during the 'new economy' boom of the 1990s, responded to and fed the growing need for cryptography, and learned that its economic power could translate into influence in Washington, even against the established and entrenched national security-law enforcement opposition, as well. Joined by groups of civil libertarians who valued cryptography not only for its ability to protect privacy but also as a form of free speech, they were able to push their agenda simultaneously in the courts, in Congress, and in the media, armed with economic and civil liberties arguments as well as the ultimately pragmatic justification that the export controls no longer offered any significant national security payoff. Eventually, after a long and vicious fight, cryptography would break free of most of its government-imposed fetters.

### *Pretty Good Privacy (PGP)*

PGP marked a new dimension in the ongoing battle between the NSA and the cryptographers outside the Triple Fence. In the previous two decades, the NSA had devised two major methods of dealing with its 'adversaries': the academic community (pre-publication review, patent reviews, secrecy orders), and the software industry (export controls). In both cases, the government had leverage over the parties in question, whether it was the ability to affect the possibility of future research or future sales. PGP and its inventor Phil Zimmermann shared neither of these characteristics. There were no published papers, no patents, and no sales, overseas or otherwise, at stake. The only leverage the government had over PGP was the threat of fines or jail time for its creator – leverage it used – but the facts of the case made even these only partially credible. In addition, because it was only software code, PGP rested somewhere in the balance between a physical object and a pure idea, and represented the worst of both worlds for the NSA. As a program, it was, like a DES chip or other physical embodiment of encryption, easily implemented. But as source code, as with an idea, it was readily transferable, easily duplicated, and absolutely irretrievable once it got loose. The release of PGP, in the end, marked the real beginning of the end for the effectiveness of export controls.

Zimmermann was a computer programmer and privacy activist of the Vietnam protest era who was infinitely paranoid about the government and its intentions. In terms of environment and timing, he realized that in the computer age, electronic surveillance would provide the government with an extremely powerful tool for monitoring dissent – or anything else. As he would later state, e-mail technology as it stood during the early 1980s was actually a step backward in the protection of privacy, because it did not even have the protection of a sealed envelope. Encryption was the answer to the dilemma.

In 1984, Zimmermann met Charlie Merritt, a fellow cryptography enthusiast who had started a small company that tried to implement RSA public key protocols on personal computers (Z-80s). Up until then, no one had successfully run public key on a PC, because the PCs of the era did not have the processing power necessary to run such programs.[148] Zimmermann realized that the speed limitations of public key (a combination of slow processor speed and bulky algorithms) meant a hybrid system of RSA key exchange protocols and some other faster encryption algorithms would be necessary. Blissfully unaware of parallel efforts at Lotus (Notes) at the time, or RSA's business model of licensing public key for similar systems, Zimmermann set to creating a program that would take advantage of network effects by running on all different types of processors, being easy to use, and easily and rapidly circulated. After six years of work, using a cipher devised by Merritt for bulk encryption and RSA for the key exchange protocol, he had come up with a workable program, which he dubbed Pretty Good Privacy (PGP).[149]

The final problem remaining was the issue of the RSA patents. Back in 1986, Zimmermann and Merritt had met with RSA's Jim Bidzos. At the meeting, Zimmermann had told Bidzos of his plan to produce a public key encryption program, and Bidzos had given him a copy of RSA's own, similar program, Mailsafe, written by Rivest and Adleman. (Zimmermann claimed he never even opened the package.) Zimmermann and Bidzos' differing recollections of the meeting would cause problems for years to come. Zimmermann claims that Bidzos was so impressed by Zimmermann's independent attempt to create an encryption system that he offered a free license to RSA; Bidzos denies this.[150] Four years later, with PGP almost ready to go, Zimmermann called Bidzos to try to resolve the RSA licensing issue, asking for the go-ahead to use the algorithm. Bidzos refused, quite understandably, since RSA made its money off licensing fees. Licensing fees, however, were completely incompatible with Zimmermann's plans for the program – a free, downloadable, shareware program where people would pay when they

[148] RSA, for example, required huge numbers, but the average PC processor at the time could only handle 8 bits at a time, which meant the standard 1024-bit keys had to be broken down and crunched 8 bits at a time. It also needed to be done quickly and efficiently, or else the program would run so slowly that no one would use it.

[149] The name was a tribute to Ralph's Pretty Good Grocery in Garrison Keillor's Lake Woebegon stories.

[150] Levy, *Crypto* 193.

downloaded, on the honor system. Frustrated, he decided to ignore the problem and go back to finishing PGP.

Then something interesting happened that would make PGP and Phil Zimmermann famous. On January 24, 1991, Senator Joseph Biden, head of the Senate Judiciary Committee, inserted some new language into a piece of pending anti-terrorism legislation, Senate Bill 266. The text read:

> *"It is the sense of Congress that providers of electronics communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law."*[151]

The specific sentence had been put in at the explicit request of the FBI. The implications of the sentence, which initially escaped scrutiny in the massive bill, were devastating for the cryptographic revolution. The point of encryption, of programs like Notes, Mailsafe, and PGP, was to ensure secure communications between the sender and the recipient, and only those two parties. The legislation, however, required that telephone companies and tech companies (software manufacturers, programmers, etc) be able to deliver the *plaintext* contents of every message, a feat logically possible only if trapdoors were built into the programs. This not only ran contrary to privacy interests, but to the very concept of secure communications. They would serve as the foreshadowing of key escrow.

The cryptographic community did not learn of the clause until April 1991, through, appropriately enough, a posting on various Internet bulletin boards. The posting ended with the suggestion "I suggest you begin to stock up on crypto gear while can still get it."[152] Phil Zimmermann took the posting as a call to arms. He needed to get PGP out before S. 266 passed and made it illegal. As a result, he abandoned his original plans to distribute PGP as shareware and decided to distribute it as freeware. For his distribution channel, he chose the most efficient means possible: the Internet. In 1991, the Internet was just starting to become popular, but it was still largely the domain of the computer savvy – or, to put it bluntly, geeks and nerds. Still, it was precisely those computer geeks and nerds who would because of ideology and technological skill respond to the program.[153]

Sometime during the course of development, Phil Zimmermann had gotten in contact with a fellow cryptography enthusiast in California named Kelly Goen and given him a copy of the PGP software. On May 24, 1991, Goen emailed a reporter at the *Micro Times*, a San Francisco Bay Area computer-oriented newspaper, and explained the purpose of flooding the Internet with PGP. "The intent

[151] S. 266, 102nd Congress, 1st session. Quoted in Levy, *Crypto* 195.

[152] Jim Warren, "Is Phil Zimmermann Being Persecuted? Why? By Whom? Who's Next?" *Micro Times*, April 1995, in Levy, *Crypto* 196.

[153] Then as today, the computer hacker community tends to be ideologically libertarian. Also, PGP then was not a particularly user-friendly program. Even the process of downloading files and installing them in such a way as to run on personal computers required a significantly above-average understanding of computers, and so the computer hacker community was the one most likely to be able to implement the program.

here is to invalidate the so-called trapdoor provision of the new Senate bill coming down the pike before it makes it into law."[154] That is, if PGP were spread across the Internet and in widespread use, the Senate bill would become moot. PGP encryption would be unbreakable, and AT&T and its cousins would not be able to guarantee plaintext even with a federal order.

In June, the reporter got a series of calls from Goen, telling him the day had arrived. Goen, clearly a little paranoid and caught up in the excitement of it all, was driving around San Francisco with a laptop, an acoustic coupler, and a cell phone, uploading a few copies for a few minutes, disconnecting, and moving to another pay phone a few miles away. "He said he wanted to get as many copies scattered as widely as possible around the nation before the government could get an injunction and stop him."[155] Goen was careful, however, to upload only to sites within the U.S., so he would not be violating any export laws. Of course, once the copies were up on the Internet on various file servers, and mirrored by dozens of other files servers in other locations and countries within hours, if not minutes, it was a moot point, since the servers were accessible to anyone around the world with a phone line, a modem and a computer. The Internet cliché was in full operation: "On the Information Highway, borders are just speed bumps." Zimmermann's intent in writing PGP was never to violate export laws; he just wanted to arm his fellow Americans with strong cryptography against S. 266. As he noted in his introduction released with the program, "When crypto is outlawed, only outlaws will have crypto."[156]

Ironically, Sen. Biden, who may not have thought through the implications of his amendment clearly and who definitely had not expected the outraged response from civil libertarians, had actually quietly withdrawn the clause in June. Unfortunately, it was too late: hundreds of thousands of copies of PGP were floating around the world, irretrievable.

Meanwhile, Zimmermann was battling RSA over patent rights while quietly overseeing a release of PGP version 2.0, with the help of much better mathematicians and cryptographers.[157] At Crypto '91, he had met with a NSA cryptographic mathematician named Brian Snow and a colleague of Adi Shamir's

[154] *Ibid.*

[155] *Ibid.*

[156] *Ibid.* 198.

[157] RSA's Jim Bidzos accused Zimmermann of stealing the RSA patent without paying licensing fees, a theft of intellectual property. Supposedly, during one of their meetings, they came to an agreement: Zimmermann would stop distributing PGP with RSA protocols, and Bidzos would not sue him. Unfortunately, mirroring the communications disconnects of their conversation in 1986, each left with a very different interpretation of their conversation. Zimmermann interpreted this to mean he could not distribute PGP anymore, without requiring him to catch all the copies that had gotten loose. Bidzos took it to mean he had to actually kill all the existing copies of PGP. (Zimmermann also claims that Bidzos agreed to sell RSA licenses to all of PGP's users so they wouldn't be in violation of the patent.) Zimmermann, on the other hand, had a rather ingenious interpretation of "distributing" PGP. As far as he was concerned, if he didn't upload any copies, he was not distributing. Bidzos, quite naturally, saw the matter differently.

named Eli Biham, who had informed him that the encryption algorithm he had written was weak – it was, for example, vulnerable to a differential cryptanalysis attack, the T attack that IBM researchers had discovered in their development of DES more than a decade ago. Zimmermann sought out the help of volunteers around the world who had been excited by the release of PGP 1.0, a motley collection of people from New Zealand, Holland, and California. They decided to use a Swiss algorithm called IDEA (International Data Encryption Algorithm), an internationally respected algorithm written by two celebrated mathematicians that had stood up to public scrutiny. Zimmermann actually considered the algorithm stronger than DES, especially with the recommended 128-bit keys. (Standard for DES was 56 bits.) PGP 2.0 also featured a new and improved key certification system, a better interface, and a number of other improvements, including translated interfaces in several languages. In September 1992, PGP 2.0 was uploaded to the Net by two of Zimmermann's collaborators in Amsterdam and Auckland – and imported *into* the U.S., so that no export laws would be violated. The new version quickly supplanted the first one.[158]

This new version only fueled the patent war with Bidzos, an argument that would not end until 1994, when Zimmermann, at the instigation of some MIT professors, took advantage of a change in RSA licensing to build RSA into PGP legally and thereby avoid a lawsuit.[159,160] Zimmermann would later face a different lawsuit, one brought against him by the Department of Justice (DOJ), which began investigating him for violation of export control regulations for posting PGP on the Internet. After the

[158] Levy, *Crypto* 203.

[159] Originally, when PGP was released, Jim Bidzos did not think that there could be any value in distributing a noncommercial, free version of a program. After all, RSA (and the partnership it later formed with another company that held related public key patents) was a company that sold intellectual property, and whose original value was based on the licensing of the various RSA patents. By the time PGP had been around for a few years, however, he had realized that distribution of such a version would allow academics and others to experiment with the RSA algorithm, so RSA released a version called RSAREF (RSA Reference), distributed by anonymous FTP and including a patent license allowing use of the patents in noncommercial programs.

Another motivation behind the release of RSAREF was the new Privacy Enhanced Mail (PEM) standard had been completed a few weeks before the first release of PGP 1.0. However, the lag time between establishing the standard and producing workable applications had given PGP a year's head start, thereby allowing it to capture the market. In addition, one of the conditions of adoption of PEM was that RSA had to create a "freely redistributable implementation of the standard that could be used royalty free for noncommercial purposes," which would allow anyone to create a noncommercial program that used the RSA algorithms.

MIT got involved when Jeff Schiller, MIT's network manager, and James Bruce, a professor and VP for information systems, suggested to Zimmermann that he use the RSAREF 2.0 encryption engine and drop it into PGP. Since RSAREF included a license for use of the RSA algorithm, the license would apply to PGP, and the patent issue would be over. Zimmermann, who had realized legitimizing PGP was the only way to expand PGP's usage, agreed. In early May, MIT's Schiller would send out a message on the Internet, which spread rapidly via the Cypherpunk and other mailing lists, announcing that MIT would shortly begin distributing PGP v. 2.5, which utilized the RSAREF engine and RSAREF 2.0 license. A few more weeks of negotiations with RSA's Bidzos, who clearly had never intended for this use of RSAREF, resulted in the version (2.6) that was eventually distributed by MIT. (It was not interoperable with previous, RSA-patent violating versions of PGP, which would force users to upgrade.) See Simson Garfinkel, *PGP.* Cambridge: O'Reilly and Associates, 1995, 103-8, for account.

[160] Because the RSA patent was valid only in the U.S., international users were not in violation of any intellectual property rights.

grand jury investigation, the case would drag on for three years without charges ever formally being brought against Zimmermann. Eventually, in January 1996, the Department of Justice dropped its case against Zimmermann. There were simply too many legal ambiguities: first, whether posting code on the Internet where foreigners can access it constitutes export or free speech/ right to publish. On the evidentiary side, Zimmermann had not actually posted the code himself; his friend Goen had. Secondly, Goen had made sure to post only to sites within the U.S.. And perhaps most importantly from a public relations standpoint, MIT had gotten involved.

PGP had gone mainstream, and the ongoing fights over cryptography and privacy had attracted plenty of attention in the media. It had also attracted a new, and more 'establishment' audience. The *Wall Street Journal* reported that lawyers were using PGP to protect client confidentiality, authors were using it to protect works in progress against copyright infringements, and professors were using it to protect their rights to ideas in unpublished materials.[161] It was becoming harder and harder for the government to argue that encryption was the domain of criminals and terrorists, and that it should be restricted. By 1994, PGP had won over its biggest ally yet: MIT. Beginning in 1994, the biggest distributor of PGP was MIT.[162] Professor Hal Abelson, of the Electrical Engineering and Computer Science department, and network manager Jeff Schiller decided that MIT should be allowed to provide Americans with programs they were legally permitted to use—and to do so on the Internet, the most efficient means of distribution. MIT stored the latest versions of PGP on its servers and allowed anyone to download it—after checking "yes" in the "Are you a U.S. citizen?" box. This was clearly not what the government had in mind, but the 'citizenship restriction' was enough for MIT to avoid prosecution, if not the displeasure of the NSA.[163] Yet at meetings between NSA counsel Ronald Lee and Schiller in 1995, the NSA refused to clarify or even provide minimal guidelines for whether MIT's restrictions were sufficient.

In a further show of support for Zimmermann, MIT Press published the code of PGP in an Optical Character Recognition (OCR) font and sold the 600-plus page book through its usual worldwide distribution channels.[164] In the words of Whit Diffie, co-inventor of public key, "Had the government prosecuted Zimmermann and not gone after MIT, it would have invited scorn. But MIT is three times as

[161] Thomas E. Weber, "Should Only the Paranoid Get E-Mail Protection? --- Probably Not, As `Encryption' Gets Easier," *The Wall Street Journal*, 25 September 1997, B6; William M. Bulkeley, "Cipher Probe: Popularity Overseas Of Encryption Code Has the U.S. Worried --- Grand Jury Ponders if Creator `Exported' the Program Through the Internet --- `Genie Is Out of the Bottle'", *The Wall Street Journal*, 28 April 1994, A1; also Levy 289.

[162] Zimmermann had licensed the PGP code to a company called ViaCrypt in an attempt to lure commercial customers, since most corporations will not use software that lacks a company to back it up and provide user support.

[163] NSA's displeasure was probably justified: MIT versions of PGP were spotted outside the country within two days of the first upload.

[164] OCR fonts can be readily scanned and converted into code with a personal scanner, available at any computer supply store for less than $100.

old as NSA, just as well funded, and even more influential in the military-industrial complex. The Department of Justice let the case drop."[165]

It had taken fourteen years since the invention of public key, but with the first upload of PGP in 1991, the encryption genie was well and truly out of the box, and there was no way for anyone to put him back in. The government hadn't seen PGP coming, but even if it had, without patents to block, papers to classify, or international sales or uploads to forbid, it is not certain the government could have done anything to stop PGP's release, much less its spread. As Steven Levy, a writer for *Wired,* writes: "Despite not being an accomplished cryptographer with a Stanford or MIT pedigree, despite having virtually no sense of business or marketing, Zimmermann had done what neither the original world-class public key mathematicians nor the market-savvy Bidzos had succeeded in doing: create a bottom-up cryptographic phenomenon that not only won over grassroots users but was being described as the major challenge to the multibillion-dollar agency behind the Triple Fence."[166] If anything, each of Zimmermann's weakness had amplified his success: his failings as a cryptographer had brought in the international cryptographic community to help, thus giving them a stake in the success of the program; his lack of exposure to the Stanford-MIT world had kept him from being derailed from his efforts by existing software (Mailsafe); while his failings as a businessman – who gives away seven years of work for free? – would make possible the rapid spread of his program and take away a critical piece of leverage the government used to control cryptography (export licenses and patent reviews). The Internet age had arrived, and for all intents and purposes, the government's export controls and other restrictions on encryption were now useless. Unfortunately, it took the government another eight years to realize it.

### *Crypto Anarchy and the Cypherpunks*

PGP was a grass roots effort undertaken for the express and conscious purpose of undermining and circumventing government control over cryptography. It was first step in a movement that was made possible by the organizing and communications possibilities of the Internet, which brought together a diverse but ultimately effective coalition of cryptographers, civil libertarians, academics, geeks, paranoiacs, and the software industry, each of which had a stake in keeping strong cryptography strong and widely available. In theoretical terms, the Internet lowered the costs of organizing to defeat the collective action problem posed by the diffuse costs to the general public of encryption controls relative to the concentrated benefits to the NSA and FBI. The ideological leanings of the civil libertarians – including Phil Zimmerman and other individuals who would come to be known as Cypherpunks – supplied the necessary incentives and different valuations of the good needed to provide leaders and

[165] Diffie and Landau 206.
[166] Levy, *Crypto* 204.

organizers for the movement.[167] When combined with the already strong incentives of the software industry, which bore significant costs due to the export restrictions, the alliance of grassroots and industry would eventually prevail. The use of the Internet also had another benefit: it made disseminating information and focusing media attention infinitely easier. As the independent cryptography community had discovered in the 1970s and 1980s with the Davida and Nicolai patent impoundments and the Poindexter Directive, media attention, particularly media attention leading to cries of 'crisis' and Congressional investigations, was the most effective way to make the NSA back down. Publicity and openness were fundamentally antithetical to the NSA's organizational ethos, so they would usually retreat in the face of the harsh media glare. The new generation of cryptography activists, more than a decade later, would not forget the lesson.

In 1992, Eric Hughes and Tim May, two anti-government mathematicians in California, decided that a community of privacy enthusiasts and hackers should be linked together to produce the tools that would enable the general public to protect themselves against cyberthieves, credit bureaus, and especially the government. They enlisted the help of influential figures in the antigovernment cryptography community. In 1990, John Gilmore, a wealthy (he had been Employee No. 5 at Sun Microsystems before he cashed out in 1986) hacker who had founded, along with Mitch Kapor and Grateful Dead lyricist John Perry Barlow, the Electronic Frontier Foundation (EEF), a lobbyist group for civil liberties in the digital age. Gilmore's pet hobby was making sure that information about cryptology found its way into the public domain. (He was the one who posted Ralph Merkle's Xerox paper on the Internet after the NSA tried to suppress it.) One result of this hobby was the filing of Freedom of Information Act (FOIA) requests to declassify four seminal early cryptanalysis texts by NSA cryptanalyst William Friedman, and hiring a lawyer to file suit when the government didn't respond within the specified legal time period. He discovered through his searches that these texts had once been declassified, then re-classified in the Reagan era, but two copies had been missed: one in the library of Virginia Military Institute (VMI), and the other on microfilm at Boston University. He had friends send him copies of the books, and informed the judge hearing the FOIA appeal that the texts were on public library shelves. The judge responded by informing Gilmore that any further distribution of the texts would violate the Espionage Act and that he would be subject to 10 years' imprisonment in a federal prison – just for checking out a book and sharing it with friends. Gilmore objected, stating that his First Amendment rights were being violated. More importantly, he called a local reporter. Two days later, the government formally declassified the two texts. (The other two, the ones not on public library shelves, remained classified.) Once again, though this time not directly targeted at the NSA, the only thing that changed government policy was media exposure.

[167] See Olson, *Logic of Collective Action.*

Meanwhile, Hughes and May were organizing the first meeting of a group (with the unfortunate moniker CASI – Cryptology Amateurs for Social Irresponsibility) dedicated to a movement that would come to be known as crypto anarchy. Unlike the nerd- and spook-fests that were the yearly Crypto conferences, the main agenda for their meetings was how people would and should use cryptographic tools. They would eventually join the software industry, privacy advocates, and reform-minded policy wonks in urging liberalization of cryptographic regulations. Perhaps the most significant outcome of this meeting, other than the coining of the new word "cypherpunks", was the establishment of a list-serv dedicated to the rants and postings of the crypto-anarchists on Gilmore's toad.com server. The Cypherpunk mailing list would soon become one of the most thorough, complete, and effective means to track not only developments in the cryptographic world, but government initiatives affecting that world. Thus, what the Internet and a few policy entrepreneurs had accomplished was the creation of a new, highly connected group of crypto-savvy, anti-government libertarians. And despite initial reluctance, they were quick to discover and exploit the power of the media, becoming media darlings and the frontier of technological cool in publications ranging from *Wired* to the *New York Times*.

### *A National Encryption Policy*

Shifting from anti-government to government activities, by the early 1990s, the need for a coherent national encryption policy was becoming obvious. By 1992, the general confusion in encryption policy was complicating the situation for the software industry and slowing the development of secure systems. Various groups sought clarification of federal encryption policy. The Computer System Security and Privacy Advisory Board, a NIST review committee created by the CSA, requested a national review of cryptography. A bill in Congress also requested a presidential analysis of various aspects of encryption policy.[168] The formulation of the policy, however, would not be a simple task. The need to satisfy several contradictory requirements –cryptography that was weak enough to export, strong enough to protect privacy, and yet had plaintext easily accessible to law enforcement with proper legal authorization – would eventually lead to the development of key escrow in the form of the Clipper Chip. In the meantime, each of the stakeholders would attempt to fortify their positions.

Just as the civil liberties activist community had linked up with the cryptographic community to further their cause, the NSA, too was recruiting allies to strength its position. Realizing that in the post-Cold War era national security claims would not have as much impact on lawmakers, the NSA had recruited allies in law enforcement circles who had a similar interest in restricting cryptography to create a coalition to push for greater regulation of cryptography. The NSA urged a national policy that would "decree [that] because of legitimate law enforcement needs in the U.S. the U.S. government will have to

[168] Clinton Brooks, Memo, April 28, 1992, in EPIC 1996, pp. C8-C13.

have a carefully controlled means of being able to decrypt information when legally authorized to do so," thus marking a slight shift in position from banning independent cryptography altogether to allowing its existence so long as it was functionally not encrypted for the NSA and government.[169] In keeping with its culture of secretiveness, however, the NSA did not want any public debate on the issue, preferring national policy to be formulated and adopted without public input.[170] In the meantime, the FBI was pursuing Digital Telephony (in all its various versions), with the NSA working on an algorithm to satisfy the FBI's need for strong but accessible cryptography, an effort that would eventually produce the Clipper Chip. The NSA would not confine its efforts to other executive agencies, however. Rather, it would also take advantage of the inexperience of the incoming Clinton administration, which after 12 years of Republican leadership had no long-standing policies on encryption to adhere to, making them ripe for conversion to the NSA-FBI vision.

Beginning in 1989, while seeking a solution to the encryption dilemma, the NSA's Clint Brooks and NIST's Ray Kammer realized that encryption would have a profound effect upon law enforcement, particularly for their ability to perform wiretaps. They began going to law enforcement, especially the FBI and DOJ, and explaining that wiretaps would be useless when criminals began encrypting their communications. Encryption was not even on the radar screen for the FBI and DOJ, and once they understood the issue, they were horrified. The NSA had found a new ally, and one whose organizational mission fit in nicely with not only the NSA's but with the political sensitivities of the time. After the Cold War, dire warnings of national security threats might not have the same appeal to Congress, but criminals were still criminals, and no lawmaker would want to appear to be soft on crime. In time, the FBI would actually come to adopt the most hard-line position on encryption of all of the national security-law enforcement agencies.

After the NSA had brought the FBI and DOJ on board the anti-cryptography agency coalition, it let the FBI take the lead in lobbying on encryption issues. The NSA was perfectly content to cede the role, since it saw its function as providing technical background and intelligence, not policy advocacy.[171] That is, it was happy to let someone do the fighting for it, as long as they were arguing for the 'right' policy; the public exposure and scrutiny necessary to become a policy advocate were simply antithetical to the organizational ethos of the NSA. Certainly the past two decades experience with public exposure – the Davida and Nicolai patent fiascos, the Congressional investigations into the NSA-NIST MOU and the Computer Security Act – had soured the NSA on publicity.

[169] *Ibid.* C12.

[170] See letter from NSA Director to Dr. Willis Ware, chair of NIST's CSSPAB, stating that "The National Security Agency has serious reservations about a public debate on cryptography." Cited in John M. McConnell, Letter to Willis Ware, July 23, 1992, in EPIC 1995a, p. C-14, in Diffie and Landau 207.

[171] Levy, *Crypto* 240.

The one exception to the anti-publicity stance of the NSA was Clinton Brooks, the Assistant to the Director. Brooks *wanted* a national debate on cryptography and key escrow, because he had come up with a solution to the encryption dilemma. He had figured out a way to resolve the contradictions of the public's need for strong encryption and the NSA's need for plaintext traffic: key escrow. Brooks compared it to a search warrant in the physical world that forced a criminal to give up the combination to a safe. The key escrow system would be the digital equivalent, storing a duplicate set of keys somewhere safe – *in escrow* – where only someone with legal authority, in the form of a search warrant or a set of national security criteria, could access the key. Then, Brooks reasoned, encryption could be as strong as anyone liked. Of course, the obvious problem with this analogy, and ultimately, the fatal flaw in the plan, was that in the real world, there was no escrow facility where safe combinations were kept. If the criminal invoked his Fifth Amendment rights and refused to reveal the safe combination, the authorities could only hold him in contempt or try to crack the safe themselves; they would not be able to bypass him and go retrieve the combination from somewhere else. It was this point that critics of the Clipper Chip plan, as it came to be known, would emphasize.

The Clipper program was sought to use standardization and federal buying power (they seeded the market hoping to create the critical mass necessary to start the network effect) to influence civilian use and choice in cryptography.[172] The NSA and FBI hoped that by establishing a federal standard, it would force individuals and industries that needed to deal with the federal government to adopt the same protocols to ensure interoperability, while not adopting other systems, as running two standards within the same company would be too inconvenient. As the initial group of companies doing business with the government grew, the network effect would kick in, creating a snowball effect whereby the Clipper Chip would become a de facto national standard, eliminating other standards, even though the Clipper Chip was technically voluntary.

Still, Brooks recognized that putting in a secret back door would be an absolute disaster if the public – or the media – were to ever find out. He believed that only with a national debate could escrow be established, because key escrow required such an elaborate infrastructure and required public acceptance and compliance for it to be feasible. The NSA top officials were absolutely horrified. Brooks explained: NSA had to collaborate with the general public. They *needed* key escrow to preserve their abilities in the future, but the judgment couldn't be made by the NSA director or a committee of deputies, because it was a *value judgment* about what was best for the national interest, and the way American politics works, value judgments are the domain of elected officials – especially the President. "His peers thought he'd gone off the deep end. *This was the National Security Agency,* their attitude was, *and we don't do that sort of thing* [italics in original], " writes Steven Levy. What Brooks' realization did do,

[172] Diffie and Landau 208.

however, was to set the course for the NSA-FBI lobbying – and eventual capture – of the new Clinton administration.[173]

*1992 Digital Telephony, Round 1*

In 1992, the FBI's Advanced Telephony Unity (wiretapping unit) predicted that because of encryption, only 60% of intercepted communications would be readable. Their worst-case scenario was 0% access by 1995.[174] The 1992 breakup of AT&T had complicated wiretapping for the FBI. It now had to deal with dozens of telephone companies, rather than a single one, and a variety of different types of equipment for different services.

The FBI put forth a proposal (Digital Telephony) that required that telephone switching equipment be designed to ease authorized wiretapping. The proposal also required that telephone companies and private branch exchanges (PBXs, the switchboards used in large companies) design their systems to accommodate government interceptions within 18 months (36 for private companies), with costs borne by the companies.[175] The FBI claimed that the new switching technologies and technologies such as cell phones and call forwarding had made it difficult to install court-authorized wiretaps. Essentially, the FBI asked Congress to make the problems go away. However, the FBI could produce no evidence of this difficulty. At the same time they claimed to Congress that technology was hampering their wiretapping abilities, they told the *Washington Post* that they "have not yet fumbled a criminal probe due to the inability to tap a phone."[176] The FBI's explanation of the contradiction was that *anticipated* technological problems had kept them from seeking or executing court ordered wiretaps. FOIA litigation filed by the Computer Professionals for Social Responsibility, however, could not find a single example of wiretapping being foiled by technology.[177]

In any case, the telephone, computer, communications and other affected industries (large companies with PBXs) protested the cost (estimated at over $2 billion) and the loss of privacy, since built-in backdoors could facilitate illegal surveillance.[178] Congress, too, rejected the bill, with no one

[173] Levy, *Crypto* 231.

[174] Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview" briefing, 1992, cited in Diffie and Landau 183.

[175] FBI. "Digital Telephony Proposal." In CPSR 1993, in Diffie and Landau 184.

[176] John Mintz, "Intelligence Community in Breach with Business," *Washington Post,* April 30, 1992, A8.

[177] All in Diffie and Landau 184.

[178] Estimates by the U.S. Telephone Association, cited in Roy Neel, President of the U.S. Telephone Association, in United States Senate, Committee on the Judiciary, Subcommittee on Technology and the Law (Senate), and United States House of Representatives, Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services,* Joint Hearings on HR 4922 and S. 2375, March 18 and August 11, 1994, 103rd Cong., 2nd Sess., 53-64, and United States House of Representatives, Committee on the Judiciary, *Report on Telecommunications Carrier Assistance to the Government,* HR103-827, 103rd Cong., 2nd Sess., 53-64.

stepping up to sponsor the proposal, despite intense lobbying by the FBI: too many outside evaluators objected. The GAO's briefing to Congress worried that alternatives to the proposal had not been explored or evaluated.[179] The General Services Administration described the proposal as unnecessary and potentially harmful to the nation's competitiveness.[180] And in an internal government memo, the National Telecommunications and Information Agency pointed out that making government interception easier would also make unauthorized, illegal interception easier as well, describing the proposal as "highly regulatory and broad."[181] Apparently, the FBI did not think the measure would pass when it was submitted, either; their internal memoranda show a 30% chance.[182]

In addition, it was an election year, and such controversial and complicated issues were politically inconvenient during the election year. Brooks figured that the George H.W. Bush people were simply reluctant to tackle such an issue during an election year, so he held off, figuring that next year, when the Bush people were back, they'd work on it again. Unfortunately, two minor problems came up: first, the introduction of the TSD3600. Secondly, Bush lost.[183] This election results would set the stage for a whole new round of lobbying by both the national security establishment and the software industry.

*TSD3600 and the Clipper Chip*

During the 1980s, secure telephones had become commonplace in the national security community, with AT&T, Motorola and Lockheed Martin each producing versions of the standard STU-III secure telephone. Each of these devices was large, clunky, expensive, and generally not interoperable with other models. By late 1991, however, AT&T engineers had figured out how to make a mass market secure telephone that was relatively inexpensive, highly effective, and easy-to-use: the TSD3600. The NSA, along with the FBI and NIST, had been largely focused on encryption in computers, so the TSD3600 took them by surprise. They quickly recognized that secure telephones using DES, the controversial, too-powerful algorithm that the NSA now regretted ever approving, would pose enormous obstacles for law enforcement. To stave off the AT&T phone, the FBI had to come up with a solution, and quick, before the units shipped. It was time for the Clipper Chip.

On October 13, 1992, Judge Sessions, the Director of the FBI, called AT&T's chief executive, Robert Allen. He explained the problem and offered a solution: would AT&T replace DES with escrowed

[179] US-GAO. *Advanced Communications Technologies Pose Wiretapping Challenge*, Briefing Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives, July 1992, in Diffie and Landau 184.

[180] US-GSA, Attachment to May 5, 1992 GSA memo, p.2, in CPSR 1993, in Diffie and Landau 184.

[181] National Telecommunications and Information Agency, "Technological Competitiveness and Policy Concerns," 1992, in EPIC 1994, from Diffie and Landau 184.

[182] Lynn McNulty, Memo for the Record, August 18, 1992, in EPIC 1996, C14-C19.

[183] Levy, *Crypto* 235.

encryption chips? Sessions offered several inducements: first, that AT&T could claim that it was providing stronger encryption, since the Skipjack algorithm was more powerful and difficult to crack than DES. Second, the U.S. would probably allow export of the escrowed phone. And lastly, the federal government would order thousands of phones for its own use, thereby ensuring sales and the continued goodwill of the U.S. government (at a time when AT&T was negotiating a $10 billion contract on a separate issue), as well as a considerable advantage if Clipper were adopted as a government standard. It was too much to resist.[184] Allen agreed, and the NSA promised that it would deliver the chips for this scheme by fall of 1992 to fit into the delivery schedule of the project. The chips did not arrive on schedule, and sample TSD3600s were produced using the DES algorithm instead in fall 1992. AT&T promised the NSA-chip version would soon join the product lineup.[185]

### *The Clinton Administration and Clipper*

The tides were turning against the government, in terms of the evolution of the public's view of cryptography and the forces allied against restrictions. The NSA's Stewart Baker soon realized that the government needed another solution. They could not mandate what people in the U.S. could use; they couldn't keep PGP away from every computer geek with an Internet connection. But realistically, most people weren't going to go through the bother of finding programs like PGP and learning how to use them. Thus export controls were the only real large-scale solution for keeping strong cryptography away from the bad guys, except Congressional support for export controls seemed to be waning. The software industry had grown up in an environment with relatively few regulations, and now it had become a multi-billion dollar colossus with plenty of pull in Washington and a libertarian attitude that believed the government should just let the marketplace figure things out. The NSA disagreed. They believed that the techies just didn't understand the real world, didn't understand why cryptography was classified as a munition. They believed the techies, like most of the American public, simply didn't understand how critical the ability to eavesdrop on the world was to American defense policy. They didn't understand what those vague reports of 'intercepts' that allowed the U.S. to catch the Libyan terrorists from the Lockerbie bombing, monitor North Korean development of nuclear weapons, and keep an eye on Iraq really meant – and they didn't know, because it was all heavily classified material, and there was no way to let them know. Encryption should be an important part of the information age, Baker believed, but he also believed that controls, to make sure the NSA could continue to eavesdrop on the bad guys, were necessary.[186]

[184] *Ibid.* 238.
[185] *Ibid.* 237, Diffie and Landau 208 for account of inserting escrowed chips into TSD3600.
[186] Levy, *Crypto* 241-2.

The NSA and FBI set about convincing the new Clinton administration of the necessity of key escrow even before the Clinton people arrived in Washington, and they were quite successful. FBI Director Judge Sessions, in particular, fearful of losing his wiretapping ability when the TSD3600s shipped, was fearless and persistent in lobbying the incoming administration. The coalition had a particularly useful convert in Al Gore, who as a technology lover was able to appreciate the ingenuity of the Clipper scheme. The NSA and NIST cooperated to anticipate and head off possible objections, including putting together a team of outside cryptographers with security clearances to validate the Skipjack algorithm, which the NSA insisted on keeping secret. The flurry of briefings and memos continued, each presenting a stacked deck of dire options. The first option: do nothing, let the market run its course, and you'll have crypto-anarchy, with AT&T selling its DES phones and cryptographic software everywhere, dirt cheap from high production volume, and when the next terrorist bombing happens, the government won't be able to stop it because the terrorists were able to communicate with unbreakable encryption. The second option, offered by the law enforcement hardliners, including Louis Freeh, Director of the FBI, was to ban any non-escrowed encryption, even within the U.S.. Anyone who needed cryptography that badly would find a way to get it, they reasoned, especially since it *was* so readily available. Thus it should be banned, just as nuclear weapons were banned, just in case the bad guys tried to get hold of it. The Clinton team, however, knew full well that this second option was a no-go; besides the dubious Constitutionality of the proposition, the software industry would never allow it.[187] After these two unpleasant options, the law enforcement-national security coalition would present the Clipper chip option, which sounded quite reasonable by comparison.[188]

The national security-law enforcement agency coalition presented the Clipper Chip scheme to the Clinton administration as ready to go. They hinted that hesitation and temporary inaction would result in a severe and lingering disrespect from the national security-law enforcement community whose endorsement the administration needed. (Clinton had been viewed as weak in national security and law enforcement during the campaign, and his lack of service in Vietnam had been a constant point of criticism.) By the time the Clinton administration took office, the original NSA-FBI lobbying team, which now had expanded to include the CIA, DOJ, and to a lesser extent, the NIST. Though they were ostensibly briefing the new Clinton administration, what they were really doing was steering it inevitably and firmly toward endorsement of Clipper. Barely a month into the White House, the Clinton administration had mentally shifted away from consideration and toward implementation. The Clinton administration had come to identify their interests with those of the national security-law enforcement

[187] *Ibid.* 243-4.

[188] One Clinton insider, in retrospect, compared it to the options presented to Kennedy on the invasion of Cuba: a cowardly avoidance of the problem; a destabilizing full-scale military operation; or a little operation at a place called the Bay of Pigs. In Levy, *Crypto* 245.

community whose approval the administration needed, to the exclusion of all other viewpoints, including those of the software industry, which could not even get in to meet with Clinton staffers. It was a classic case of regulatory capture, only by a government agency rather than industry. The impending shipment of 10,000 AT&T DES-equipped TSD3600s on April 1 heightened the sense of urgency, and memos urging completion of the Clinton administration's first major initiative, urging "closure", flew. The coalition's classified briefings, ingeniously presenting the tradeoff as 'If you do nothing, people will die. Do you want to sacrifice human lives for a 0.1 percent increase in GDP?', had done the trick. Thousands of people dying versus Bill Gates being a few million dollars richer. It was not a tough choice for the administration.[189]

Barely three months after taking office, on April 16, 1993, the new Clinton White House announced the Escrowed Encryption Initiative, a federal standard that was intended to "improve security and privacy of telephone communications."[190] The standard was to use a classified algorithm (Skipjack) put on tamper-proof chips (Clipper) manufactured in a secure facility (by Mykotronx in California, a defense contractor) with escrowed keys. Key escrow meant that copies of the encryption key were kept by the government. When the chips were manufactured, escrow agents would be present. The key itself would be split into two components, with each piece stored at a secure facility controlled by a federal executive branch agency, following the two-person security protocol used for nuclear devices. Both keys would be necessary to decrypt messages.[191] (Brooks had originally argued that, like the public debate over implementation of the Clipper Chip, the algorithm, too, should be released for public scrutiny, but the NSA absolutely refused. To the NSA, it would amount to showing the world the cutting edge of NSA's cryptography research – and that simply wasn't how things were done at The Fort.)[192]

The proposed standard would be limited to encryption of voice, fax, and computer information transmitted over a telephone system.[193] The Clinton administration stated at the announcement of the Clipper chip proposal that it was not prohibiting encryption outright, but neither was it acknowledging the

[189] *Ibid.* 246-7.

[190] See http://www.nist.gov/public_affairs/releases/n94-08.htm for text of NIST press release.

[191] The operation of the Clipper chip reflected this split duplicate key. When a Clipper Chip begins encrypting a message, it first sends out a signal called the Law Enforcement Access Field (LEAF). This signal must be received by the Clipper chip doing the decrypting. The LEAF is linked to the encryption key used, so that both must matched for a message to be decrypted. The LEAF could only be decrypted by a special government-held key unique to that particular chip (the first half of the escrowed key). That message would then reveal the identity of the unique Clipper Chip and its associated encryption key (the other half of the escrowed key).

[192] *Ibid.* 232.

[193] United States Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard," *Federal Register,* Vol. 59, No. 27, February 9, 1994, 6003.

right to unbreakable commercial encryption.[194] The administration would later state that it would not seek legislation limiting the use of encryption.[195]

As required by law, the NIST provided a period for public comments on the Clipper Chip proposal. The response was overwhelmingly negative, with opponents ranging from the ACLU to Citicorp to a large portion of the computer industry. Of the 320 comments received, only two agreed with Clipper, and one was from Motorola, which planned to manufacture phones using the Clipper Chip. "This is not a Hall of Fame batting average," noted NIST official Lynn McNulty.[196] Even government agencies, including the Department of Energy, United States Agency for International Development (USAID), and Nuclear Regulatory Commission opposed the Clipper Chip; the others who bothered to comment at all had "no comment."[197] The Clinton administration, or more specifically the NSA and FBI coalition that had come up with the idea for the Clipper Chip, had managed to alienate just about everyone with any stake in the issue. As an example of the level of opposition, an Internet petition based on a January 1994 letter written by the Computer Professionals for Social Responsibility to the President urging him to rescind the Clipper proposal, a letter originally signed by privacy experts, cryptographers, industry figures, and academics, received over 47,000 signatures. It was one of the first Internet petitions, and a CNN/NYT poll showed that over 80% of the American public opposed Clipper.[198]

There were several major flaws with the Clipper proposal that the Clinton administration had managed to overlook or play down. First, though the intentions were good, the entire concept of the scheme – allowing the government a back door into private communications – was fundamentally in opposition to the idea of individual privacy. Even the Average Joe would understand the analogy that Clipper was like requiring you to leave a copy of your front door key at the police station, and would with no effort at all become an anti-Clipper convert.[199] The very design of the Clipper Chip system inherently lowered privacy even if the escrowed keys were never used. The simple existence of the technical ability, and therefore the possibility, of communications being read created an (accurate) perception that no communication was truly private.

Second, the reason some people wanted cryptography was to keep information from the government. It was not because they were criminals; it was because they simply didn't trust the

[194] The White House, Office of the Press Secretary, "Statement on the Clipper Chip Initiative," in EPIC 1994, April 16, 1993.

[195] USDoC 1994, p. 5998; John M. McConnell, Testimony in United States Senate, USS 103, 102, cited in Diffie and Landau 211.

[196] Steven Levy, "The Cypherpunks vs. Uncle Sam," *Sunday New York Times Magazine,* June 12, 1994.

[197] Diffie and Landau 212 and footnotes.

[198] Philip Elmer-Dewitt, "Who Should Keep the Keys?" *Time,* March 14, 1994, cited in Levy, *Crypto* 261.

[199] *Ibid.* 251.

government.[200] To create a system where the very government they were trying to encrypt their communications against was simply absurd.

Third, key escrow was also a step backward in terms of technological innovation. The revolutionary aspect of public key cryptography in the 1970s was that it enabled secure communications among users without the need for a centralized key authority that would be a natural target for criminals and eavesdroppers, the problem that had plagued symmetrical key systems. Key escrow by its very nature *created* such a central key management facility, thereby providing a large and obvious target.

Fourth, key escrow, by creating fixed keys that would be used for the lifetime of the chip (or rather, the device, since the chips were built in), would increase vulnerability and reduce security. The reason one-time pads are the only mathematically unbreakable encryption system is because they are only used once. The longer a single key is in use, the more incentive and opportunity a hacker has to attempt to break it. Modern encryption technology of the time had already begun using session keys, keys that were used only once or for a limited number of uses, thus limiting the quantity of encrypted text that could provide data for breaking the key, as well as limiting the utility of breaking the key.

Fifth, the manufacturing process, because it was dependent on production of the chips by a government contractor unaccustomed to commercial production, slowed down innovation in the communications industry and interfered with industry. The presence of the LEAF and the need for key escrow naturally required that the Skipjack algorithm be put in a tamper resistance chip. However, using a *classified* algorithm in a federal standard was highly unusual. The purpose of having federal standards is to promote interoperability. By including a classified algorithm, the federal government turned the standard into a means for controlling both the industry and the final end product. Normally, the way a federal standard works is the standard and its specifications are published. The manufacturer reads the standards, develops a product conforming to them, and submits the product for certification. The Clipper Chip system forced government involvement in supply, development, and approval, rather than only the final step. Thus the company would be dependent upon the government from start to finish, even in future production (for more parts to continue a product line). Not only could manufacturers only buy from government-designated sources of the chips, they needed government permission to buy the product at all, thereby giving the government significant leverage over industry. The government stated openly in the Escrowed Encryption Standard (EES) documentation that it would regulate which companies would be allowed to include the new Clipper Chip in their products. Critics feared not only the infringement on industry's freedom of product development, but the bureaucratic hurdles that would slow down the usually fast-moving, innovative computer industry.[201]

[200] *Ibid.* 252.

[201] Diffie and Landau 213.

Sixth, the government couldn't answer the simple question of who would actually use the Clipper chip, knowing that it meant the government could eavesdrop. The government's best answer had been the 'stupid crook theory,' an idea explained best by the FBI's Jim Kallstrom, who told of hearing wiretaps in which mobsters joked about being wiretapped and kept talking anyway because they were too lazy to go outside and use a pay phone. Kallstrom's argument was that in five years, if Clipper caught on, no one would remember that the government had the ability to listen in, and criminals would just buy the devices with the Clipper built in.[202] Unfortunately, Kallstrom had no answer to the question of what smart criminals – or people from other countries – might do as an alternative.

Despite all of these shortcomings and all of the criticism, the standard was adopted on February 9, 1994. It was an unmitigated failure. With the exception of 9,000 phones ordered by the FBI in an attempt to seed the market, very few were purchased, and no company other than AT&T made any Clipper phones. It was a voluntary standard, but critics argued that it was a first step toward non-escrowed encryption, a statement borne out by earlier FBI statements that they would seek a federal ban on non-escrowed encryption if necessary. NIST also stated that they hoped the Clipper Chip would, by becoming a federal standard, replace non-escrowed encryption and make non-escrowed encryption harder to obtain. NSA also attempted at the last minute to modify the regulation from covering "telephone communications" to "telecommunications systems" and PCMCIA cards, a step that would have turned EES into the standard for voice and data communications.[203] The inclusion of PCMCIA cards was NSA's attempt to circumvent the approval process for Fortezza, a NSA-developed PCMCIA card containing an encryption system for key exchange, digital signatures and data encryption using the Skipjack algorithm. These changes were withdrawn only after protests from NIST scientists.[204]

Four months later, an obscure cryptology geek put the last nail in Clipper's coffin. Matthew Blaze, an AT&T research scientist from New York, was hired by the NSA as an outside analyst to evaluate Tessera, the smart-card (PCMCIA) version of the key escrow system. He decided that rather than attack the Skipjack algorithm, which the NSA itself had certified as unbreakable and a million times more powerful than DES, he would try to find a way to defeat the escrow feature (LEAF). He used a card reader and a program that simulated a wiretap, and after a while, discovered the LEAF checksum (the feature that verifies the chip identifier and session key to the authorities) was only 16 bits long. All he needed was a way to produce a legitimate checksum with a fake LEAF, and the authorities would receive a message that would supposedly lead to the correct key but actually led nowhere – and he would have a message the authorities couldn't retrieve, encrypted using the powerful Skipjack algorithm. Sixteen bits

[202] Levy, *Crypto* 255.
[203] United States Department of Defense, National Security Agency, Office of General Counsel, "Proposed Changes to Escrow Encryption Standard," January 12, 1994, in Diffie and Landau 214.
[204] Diffie and Landau 214.

was not much by 1994. Blaze rigged a program that would use a brute-force attack on the checksum, all $2^{16}$ possible combinations, and dubbed it the "LEAF blower." It took 42 minutes to defeat the system. Blaze even found a way to defeat the system more quickly when both Clipper users worked together. Surprisingly, when he sent his results to the NSA, they did not object. Neither did his superiors at AT&T, even though they had millions of dollars riding on the Clipper phones.[205] John Markoff of the *New York Times* had obtained a copy of the paper from Blaze, and the next morning, the front page story headline ran, "Flaw Discovered in Federal Plan for Wiretapping."[206] Public trust in the system was effectively gone, even if the flaw was easily fixed. Perhaps equally significantly, the elevation of encryption to front-page news showed how much the public's awareness of the issue had grown since only a decade ago.

Nonetheless, the government continued with their attempts to push key escrow, despite the failure of the Clipper Chip initiative.[207] They did become more creative in their marketing, however. Instead of calling it "key escrow," which had become political poison, they began to push for "key recovery," marketing the concept as a way for users to recover their data if they lose their keys, and urging users not to trust cryptographic systems unless they had key recovery, since it would be a way to make sure they could get their data back.[208]

The other result of the failure of the Clipper Chip proposal was that the government fell back on the only other tool for limiting encryption that was available without yet more new legislation: export controls. Export controls had become a more attractive option, as global demand for mass-market cryptography had increased, making exportability essential for successful, profitable mass-market products, and consequently increasing government leverage over software producers.[209] The NIST issued a list of ten principles for software key escrow, compliance with which would allow export. However,

[205] Actually, some supervisors did object until Blaze managed to convince them that they would not be able to keep the results secret, especially since John Markoff of the *New York Times,* who did most of the reporting on the Clipper Chip for the *Times,* had already heard about the work.

[206] John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *NYT,* June 2, 1994. Blaze's paper on the finding the flaw in Clipper is Matthew Blaze, "Protocol Failure in the Escrowed Encryption Standard," *Proceedings of the Second ACM Conference on Computer and Communications Security,* November 1994, both cited in Levy, *Crypto* 256-61.

[207] They sold poorly, with the exception of 9000 Clipper models purchased by the FBI in an attempt to seed the market. AT&T was the only company that had ever bothered to use the Clipper Chip in its products. (Diffie and Landau 215)

[208] Executive Office of the President, Office of Management and Budget, Interagency Working Group on Cryptography Policy, Bruce W. McConnell and Edward J. Appel, Co-Chairs. *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure (draft),* May 20, 1996, cited in Diffie and Landau 217. To some extent, this is true. If all copies of a file are encrypted, and you lose your key, the files are as good as gone. However, this is not necessarily true for communications. For phone calls, key recovery will not recover or preserve the plaintext transcript of a secure phone call. For email, key recovery depends on the encryption key used for the stored text. Some users download their email, decrypt, and re-encrypt in a local storage key, as they would any other data on their hard drive. Key recovery would not be useful in this case. Only if the email is left encrypted in the transit key would key recovery serve a "data recovery" function.

[209] Diffie and Landau 208.

NIST had no role in the export approval process, and the Department of Commerce plays only a limited role, secondary to the Department of State, which defers to the NSA on encryption issues.[210] Thus, again, the NSA was functionally running the game. The main point in the "Ten Commandments" was to limit the key size of exportable cryptosystems to 64-bits on the condition they feature recoverable keys in either direction of communication. They could not interoperate with un-escrowed versions of the same systems. And most importantly, the key escrow agents had to be in the U.S. or in countries with bilateral agreements with the U.S. that would guarantee the U.S. government access to the keys.[211] Eventually, the key length restrictions and interoperability requirements were dropped.

*Digital Telephony, Round II*

The FBI's aggressive campaign to preserve the value of its wiretapping on several fronts did not cease during the period. The NSA had convinced it that a vital organizational interest was at stake, and the new FBI Director, Louis Freeh (who had replaced Judge Sessions), was if anything more emphatic and dogged in pursuing this goal on Capitol Hill. During the middle of the Clipper debate, in March 1994, the FBI re-submitted a revised Digital Telephony Bill. This time it limited its wiretapping proposals to common carriers and proposed an allocation of $500 million to cover costs. It gave the common carriers three years after the Attorney General published notification of new requirements to comply, up from 18 months. Most importantly for this study, the new Digital Telephony proposal removed responsibility for decryption from the telecommunications industry unless the carrier itself had provided the encryption, thereby removing one of the most objectionable aspects of the previous bill.[212]

In a series of appearances over the next two months, Freeh would claim anywhere from 91 to "several hundred" instances in which new technology had prevented court-ordered surveillance, though Freeh seems to have confounded electronic bugs with wiretaps (the former does not require involvement by telephone companies) in his speeches.[213] In April 1994, in response to criticisms that his examples were vague, Freeh submitted examples of 183 cases in which the FBI had had difficulty executing court-ordered surveillance.[214] The GAO confirmed that the FBI did face problems in wiretapping as a result of new digital technologies such as optical fiber, call forwarding, and ISDN.[215] After some difficulty and

[210] Authority over the export approval process was transferred from the Department of State to the Department of Commerce in 1996.

[211] *Ibid.* 216.

[212] CALEA, Public Law 103-414, Section 109.

[213] Louis Freeh, Speech to the Executives' Club of Chicago, February 17, 1994; Louis Freeh, Testimony in USS 103b, pp. 5-51; both cited in Diffie and Landau 195-6.

[214] USHR 103b, 14.

[215] *Ibid.* 14-5.

much lobbying, Freeh was able to convince Congress to pass the bill that he had made his agency's highest priority.[216] It was called the Communications Assistance for Law Enforcement Act (CALEA).[217]

Obviously, the usefulness of wiretapping ability is cut down sharply if the overheard conversations are encrypted. Perhaps seeking to prevent civil libertarians from joining up with the telephone carriers to block the bill, the FBI downplayed the connection between CALEA and encryption, and especially the connection between CALEA and the Clipper Chip, during the lobbying effort for CALEA.[218] However, when passage of CALEA looked likely, Freeh stated that if the FBI encountered non-escrowed encrypted conversations in wiretapped communications, he would go to Congress and ask for laws barring non-escrowed encryption.[219] The White House disavowed Freeh's statement as his policy and not the White House's, but in keeping with his organization's interests, Freeh continued to repeat the position in the following months.[220] This position, apparently, was the result of the FBI's efforts over the past years that the NIST had noticed in 1991. A NIST Public Key Status Report of 1991 had noted that the FBI was "working on draft legislation to control and license all cryptography."[221] A January 17, 1992 memo written by Brent Scrowcroft, National Security Advisor, stated that the President had approved the DOJ to seek a resolution to the Digital Telephony problem, and "all parties should prepare to follow through on the encryption problem in about a year... Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix, and the encryption access options can be developed more thoroughly in the meantime."[222] The beachhead had been established.

### *The Courts Weigh In*

By the 1990s, the debate over encryption had spread from obscure corners of academia and the NSA to the front pages of national newspapers, the Internet, assorted agencies scattered across Washington, Capitol Hill, and the White House. Thus far, it was not clear who was winning, the crypto-community or the government. On one hand, Digital Telephony had passed. On the other, Clipper had

[216] Sabra Chartrand, "Clinton Gets a Wiretapping Bill that Covers New Technologies," *New York Times*, October 9, 1994, A27, in Diffie and Landau 196.

[217] HR 4922, 103rd Congress, 2nd session. Became Public Law 103-414.

[218] Louis Freeh testified to Congress that "The proposed [Digital Telephony] legislation relates solely to advanced technology, not legal authority or privacy. It has nothing to do with the separate, but important, Clipper Chip technology." From Louis Freeh, Speech to American Law Institute, May 19, 1994, in EPIC 1994, p. 6 of speech.

[219] This reply to a question apparently took place during a conference on Global Cryptography in Washington, DC, in September 1994. Cited in Diffie and Landau 202.

[220] Louis Freeh, Statement to Committee on Commerce, Science, and Transportation, U.S. Senate, July 25, 1996.

[221] United States Department of Commerce, National Institute of Technology and Standards, "Public Key Status Report," in EPIC 1996, p. C-3.

[222] Brent Scrowcroft, Memorandum to Secretary of Defense Dick Cheney, Attorney General William Barr, and Director of Central Intellience Robert Gates, January 17, 1992.

failed. On one hand, PGP was widely available. On the other hand, DES was not. It was time for the great arbitrator of American society, the judicial system, to weigh in. The cypherpunks and civil libertarians, in addition to trying their cases in the media, began trying them in the courts as well. The net result, unfortunately, was as schizophrenic as the national encryption policy itself.

In *Bernstein v. United States Department of State*, the district court ruled that federal export controls on publication of encryption software code constituted an unconstitutional prior restraint on free speech. Daniel Bernstein, a graduate student at Berkeley, had written an encryption program called "Snuffle," which was based on a published hash function written by Ralph Merkle. Bernstein's program transformed the hash function into something that could encrypt and decrypt.[223] Still, in the court's decision, it reasoned that source code was "language" in that it was "the expression of ideas, commands [and] objectives," and that even though Snuffle was "essentially functional, that does not remove it from the realm of speech."[224] In the government's appeal to the Ninth Circuit Court, which dragged from December 1997 to May 1999, Bernstein's lawyer (provided by the Electronic Frontier Foundation, with John Gilmore's involvement – the same John Gilmore who had posted Merkle's Xerox paper on the Internet) argued to the Ninth Circuit that by preventing the publication of Bernstein's paper on the Internet, the government was in violation of the recent Supreme Court decision striking down the Communications Decency Act, a decision that had ruled the Internet was a beacon of democracy entitled to the highest level of First Amendment protection. When the 9th Circuit's 2-to-1 decision was finally handed down, it not only affirmed the lower court's decision, it hailed cryptography as a vital component of democracy. Wrote Judge Betty Fletcher, "Government attempts to control encryption… may well implicate not only First Amendment rights of cryptographers, but also the constitutional rights of each of us as potential recipients of encryption's bounty."[225]

Later rulings, however, would cut into the gains made by the cryptology community in *Bernstein*. In 1996, a cypherpunk named Philip Karn applied for a commodities jurisdiction (export license) to export a copy of Bruce Schneier's book *Applied Cryptography* (1994) and an accompanying floppy disk

[223] Hash functions were not subject to export controls, because they did not technically scramble information, though encryption programs were. Bernstein's Snuffle program, based on Ralph Merkle's Snerfu hash function, transformed Snerfu into something that could both encrypt and decrypt. Actually, it could transform *any* good hash function into an encryption program. As Levy explains it, "Think of Snerfu as a banned automatic weapon shipped through customs without a trigger, and the new program as a kit that installs the missing part." See Levy, *Crypto* 298.

[224] See Levy, *Crypto* 300-1. See also: Bernstein v. U.S. Dept of State, 922 F. Supp. 1426 (N.D. Cal.) (denying motion to dismiss)(partial summary judgment granted, 945 F. Supp. 1279 (1996), superseded, 974 F. Supp. 1288 (1997), in Kurt M. Saundersby, "The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff," *John Marshall Journal of Computer and Information Law*, Vol. 17, No. 945.

[225] See Bernstein v. United States Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999). For extended analysis and critique of Bernstein decision, see Patrick I. Ross, "Computer Programming Language: Bernstein v. United States Department of State," *Berkeley Technological Law Journal*, Vol. 13, No. 305 (1998). See also E. John Park, "Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security," *Virginia Journal of Law and Technology*, Vol. 2, No. 3 (1997); Levy, *Crypto* 300-2.

that contained the coded version of the algorithms printed in the book. The book itself was a compilation of cryptographic mathematical theory, explanations of various popular cryptosystems, and lots of algorithms. One crypto-community publication called it the "Bible of code hackers."[226] The State Department granted permission to ship the book, but denied permission to ship the floppy disk, even though they contained identical information. Karn challenged the decision in the courts, arguing that the Arms Export Control Act and ITAR were unconstitutional under the First and Fifth Amendments.[227] When he challenged the decision in the courts, the federal judge denied his claims and upheld the AECA and ITAR on the grounds they furthered an important or substantial national interest. He also held that, contrary to the *Bernstein* decision, ITAR did not constitute prior restraint on free speech since the regulations were content neutral. Before Karn could appeal, Clinton signed an executive order transferring jurisdiction for export controls on civilian encryption software to the Commerce Department, so the case was remanded for review under the Commerce Department's new regulations.

Two years later, another court would contradict Bernstein and follow the Karn ruling in the case of *Junger v. Daly*. Professor Peter Junger filed suit to establish that it was within his First Amendment rights to teach his "Computers and the Law" class at Case Western Reserve University School of Law and to post encryption software on his website. Given his aims at the time, it is perhaps not surprising that Junger lost his case. He wanted a permanent injunction keeping the government from enforcing the encryption software and technology provisions of the Export Administration Regulations (EAR) against anyone seeking to disclose or export encryption software. The court held that export of encryption source code on the Internet was not protected by the First Amendment, because encryption source code is "inherently functional" and the EAR were constitutional because they were "not directed at source code's expressive elements, and because the Export Regulations do not reach academic discussions of software, or software in print form." [228]

Overall, the contributions of the judicial system to the encryption debate were mixed. What the rulings did do, however, was to publicize the Constitutional rights at stake. Whereas previous attempts to restrict access to literature on encryption had been resolved unofficially, with either the withdrawal of NSA objections or with secret deals with publishers, the cypherpunks' challenges tested the export

[226] Levy, *Crypto* 289. The publication was the *Millenium Whole Earth Catalog,* which is not a natural food supply catalog as one might expect, but one of the first Bay Area newsletters for the formerly underground computer, hacker and crypto community.

[227] Karn v. United States Department of State. 925 F. Supp. 1 (D.D.C 1996), remanded, 107 F. 3d. 923 (D.C. Cir. 1997), cited in Saundersby. The First Amendment issues have been discussed. The rationale behind the Fifth Amendment claim was that by denying encryption to individuals, the individual's communications would be easily accessible in a criminal investigation, which constituted a denial of the Fifth Amendment right against self-incrimination.

[228] Junger v. Daly, 8 F. Supp. 2d. 708 (N.D. Ohio 1998), in Saundersby. For more information on the case, see "Free Speech and the Export of Crypto," http://samsara.law.cwru.edu/comp_law/crypto_export.

restrictions in public and put them on the official record. The Bernstein case, for example, marked the first time the opinion stating that ITAR and its export regulations were unconstitutional and violated First Amendment restrictions on prior restraint that the DOJ lawyer had written in 1978 – more than fifteen years ago – was tested in the courts. Thus while inconclusive, the court battles did not resolve the export control issue, they did give Congressional advocates of liberalization a valuable weapon in final debate that would take place in the last half of the 1990s.

*National Research Council Report*

Congress, which up to this point had been minimally involved in the debate over encryption, ordered an independent study into the encryption issue by the National Research Council (NRC) after the Clipper controversy.[229] The NRC was told to consider all aspects of encryption policy, including the effect of cryptography on national security, law enforcement, commercial, and privacy interests of the United States, as well as the effect of export controls on U.S. commercial interests.

The panel that produced the report consisted of 16 experts from the government, industry, and science, 13 of whom had security clearances, including a former Deputy Director of the NSA. (Three of the 13 declined to receive security clearances and so were not present for that portion of the briefing.) The report contradicted the NSA position, which argued that the public could not understand the full scope of the debate because they did not have access to classified information. Instead, the panel wrote "the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis."[230] That is, *even after hearing the classified material*, the panel decided that what they had heard was not essential for continuing the debate. The panel noted that, although classified information was often necessary for operational decisions, it was not critical to determining the evolution of cryptography policy. To add insult to injury, the panel argued for *more* use of cryptography, since "on balance, the advantages of more widespread use of cryptography outweigh the disadvantages." The report emphasized the need for "broad availability of cryptography to all legitimate elements of U.S. society." The current U.S. policy, the panel stated, was inadequate to protect the digital infrastructure of an information-based society, while the current export policies were detrimental to domestic use of strong cryptosystems.[231]

[229] Clipper was an executive decision, and the export control regime had existed for decades. The only actual legislation Congress had passed in recent years (up to 1993) was the watered-down version of the Digital Telephony Bill. And even that had so many opponents in Congress that even though the bill passed, Congress never appropriated any funds to make it a reality. During the 1980s, involvement in the debate had been limited to passing the Computer Security Act and investigating the NSA for violating the intent of that legislation.
[230] Kenneth Dam and Herbert Lin, eds., National Research Council, Commission on Physical Sciences, Mathematics, and Applications, Computer Science and Telecommunications Board, Committee to Study National Cryptography Policy, *Cryptography's Role in Securing the Information Society,* National Academy Press, 1996, 298.
[231] Diffie and Landau 300-1.

On the international side, the panel urged the government to loosen export controls, arguing that products using DES (not *escrowed* strong encryption) should be immediately made easily exportable. It urged the government to go slow with escrowed encryption until it was sure that this new technology could be adapted for large-scale use. It also argued, contrary to the NSA and FBI's stance, that "no law should bar the manufacture, sale, or use of any form of encryption within the United States."[232] To deal with the complications that encryption would present to law enforcement, the panel recommended that the government to take steps to help law enforcement adjust to the new technologies. It also recommended criminalizing the use of encryption in interstate commerce *with criminal intent,* just as using the U.S. mail to commit a crime was a federal offense. In short, the U.S. would be better off with encryption than without it – no matter what the Clinton administration thought.[233] The NRC was not what the Clinton administration wanted to hear.

### *Cypher Punks, Part II: An Epidemic of Code Breaking*

While Washington was mired in debate over encryption policy, technology, true to its nature, raced forward. The debate in Washington had raised the profile of the previously obscure field of cryptology to a national level, and a series of highly publicized hacks – undertaken by cypherpunks with the intent of turning the tide on the debate by emphasizing the need for stronger encryption as well as the inadequacies of current export laws – ensued. The activists were able to use the Internet to not only publicize their accomplishments, but to organize to make them possible. The era of distributed computing had arrived.

### *Breaking RSA-129*

In 1995, a group of cypherpunks led by a 20-year-old electrical engineering student at MIT named Derek Atkins decided to give RSA-129, the challenge offered up in Martin Gardner's 1977 *Scientific American* column, another go. It had been 15 years since Ron Rivest had offered up $100 to anyone who could factor the number and predicted it would take forty quadrillion years to do so. With 39 quadrillion-plus years to go, Atkins decided to tackle the problem.[234,235] Back when Rivest, Shamir and Adleman had come up with the challenge, they had known that new and better factoring algorithms would

[232] *Ibid.* 303.

[233] *Ibid.* 299.

[234] Rivest now says the 40 quadrillion number, based on a misunderstanding of another mathematician's evaluation of computer power at the time, was a miscalculation – but only by a few orders of magnitude, which still would have meant a few million or billion years. Rivest, clearly, had not counted on the Internet.

[235] Atkins had originally planned to try and crack PGP, which he had helped develop later versions of, but was told by Arjen Lenstra, a renowned mathematician at Bellcore Labs, that the large prime numbers used in PGP and commercial RSA would be too difficult to attack; he was the one who suggested the RSA-129 challenge.

be developed, but nothing powerful enough to break RSA in immediate future. What they did not count on, however, was the introduction of the Internet, which made it possible to harness the aggregate computing power of thousands of computers, creating a sort of Frankenstein supercomputer with parts spread around the world. Using a new factoring algorithm called the 'double large prime multiple polynomial variation of the quadratic sieve,' the hackers set to work. Between September 1993 to April 1994, the RSA-129 experiment used about 5,000 MIPS years (one year of 24/7 use of a Million Instructions Per Second machine) from computers around the world.[236] By April, Atkins guessed that enough univectors had been gathered for the final crunching, so he sent the 400MB tape to Lenstra at Bell Labs for the final matrix reduction.

Two days later, Atkins posted the message:

RSA-129 =
1143816257578888676692357799761466120102182967212423625625618429357069352457338978305
9 7123563958705058989075147599290026879543541
= 3490529510847650949147849619903898133417764638493387843990820577 *
32769132993266709549961988190834 461413177642967992942539798288533.

A bit more decoding revealed the original message, a few million (or billion or quadrillion, depending on the estimate you believe) years early: "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE."

Ron Rivest was now $100 poorer. Although RSA was still safe, since RSA-129 was the equivalent of a 425-bit key and the RSA commercial standard was 1024-bits, the implications of the successful factorization, which was not supposed to be possible within certainly Rivest's lifetime, demonstrated how even so-called strong encryption was vulnerable. After all, the government put its export cap at 40-bits – and RSA-129 was $2^{385}$ (about 8 with 115 zeros after it) times stronger than that, and it had been factored.[237]

*Netscape hacks, v. 1.0 and 2.0*

Subsequently, an attack was mounted by a similar group of cypherpunks on Netscape. Netscape used an RSA-based public key protocol called Secure Sockets Layer (SSL), built into the software so that even non-computer geek users could have the benefit of secure communications with just the click of a mouse. Soon after Netscape's $2 billion dollar IPO in 1995, a cypherpunk named Hal Finney decided to investigate Netscape's security. In keeping with export regulations, Netscape had two versions: a domestic 128-bit version using RC-4 and a 40-bit export version. Finney decided to attack the export version and coordinated with the England-based group that had organized a failed cracking attempt on

[236] For a full explanation, see http://www.math.okstate.edu/~wrightd/numthry/rsa129.html for documentation on the breaking of RSA-129. For an explanation of the algorithm, see http://www.math.uiuc.edu/~landquis/quadsieve.pdf.
[237] Factoring RSA-129 was not quite the same thing as breaking a 425-bit key, as the key contains additional elements. However, the factorization would have been the primary component of breaking that key.

Microsoft Access. He created a fake transaction (ordering an item and having it shipped to a fake address), captured the encrypted data, and included it in the challenge. A coordination problem delayed the start of the project, however, and a 27-year-old French computer scientist named Damien Doligez, at INRIA, the French government computer lab, stepped into the breach.

Doligez, being at INRIA, had access to a whole network of computers as well as a Maspar supercomputer. He quickly wrote a small program that would enable a computer to test out a potential key, and adapted it to work on the various computers on the INRIA network and some at a few nearby universities. Whenever a worker left their computer for five minutes, Doligez's program would take over the computer and begin crunching keys; touching the keyboard gave the computer back to the worker. No one minded. Ten days later – four of those due to a technical glitch that caused him to restart the search – Doligez had the key. He posted the message to the cypherpunks with the subject heading "SSL challenge – broken!", and posted the plaintext as proof. The address of the character Hal Finney had created, in a tribute to the RSA-129 crack, was Mr. Cosmic Kumquat, of SSL Trusters, Inc., 1234 Squeamish Ossifrage Road.[238]

Already in the public eye because of Netscape's massive IPO the week before, the crack generated a media frenzy. The media, perhaps missing the point, took the crack as a statement on Netscape's security. Netscape, correctly, pointed out that not only had cracking a single message taken 64 MIPS years (though Doligez also correctly pointed out that he had used only idle computer time and paid nothing for the crack), and that – more importantly for security implications – the domestic version used a much stronger 128-bit key. ($2^{88}$, or $3x10^{26}$ times stronger).

A few months later, two 22-year-old first year graduate students at Berkeley, Ian Goldberg and Dave Wagner, who had missed the brute-force attack, decided to try a different attack on Netscape. Rather than a computer-intensive brute force attack, they looked for a weakness in the SSL system. After some investigation, they found it: the Random Number Generator (RNG). The RNG is a critical piece to any cryptosystem, as it is responsible for the scrambling that ensures even the subtlest pattern disappears into a random chaos of numbers.[239] A crucial component of the RNG is the 'seed', the numbers that begin the randomization process. Usually, in a good system, this is based on a random statistic from the real world: the position of the mouse, the millionth decimal place numbers in the speed of a keystroke sequence, etc. Netscape, on the other hand, had decided to use the time, and two forms of user identification called the Process ID and the Parent ID. The first part, the time, was easy: there are only a

[238] See Levy, *Crypto* 279-81. See also Mark Tran, "Student Cracks Code on Internet Security Software: Hacker takes the gloss off Netscape's floatation success," *The Guardian,* August 18, 1995, p. 11.

[239] A lack of true randomness is one way for good cryptanalysts to break codes. This was how the German Enigma cipher was broken during WWII, because the clerks who encrypted the messages tended to use obvious three-letter combinations as their identification keys, often three letters in a row on the keyboard, e.g., "123" or "ASD".

limited number of times in the day. The second and third parts, for someone on a network that shared a server, common for an Internet environment, were also trivial. (And even if they weren't, the ID numbers were only fifteen bits long, highly vulnerable to brute force attacks, as evidenced by the 16-bit LEAF in the Clipper Chip.) Goldberg and Wagner wrote their program over a weekend. When they tested it Sunday night, it took less than a minute to find the key. They posted their results on a cypherpunk mailing list, and the story ran the next day on the front page of major newspapers.[240]

This time, Netscape couldn't blame the weakness on government restrictions. It had taken two graduate students a few minutes on a regular Pentium PC to break Netscape security. "Our engineers made a mistake," admitted Netscape's VP of marketing.[241] The one upshot was that Netscape immediately fixed the exposed weakness, lending strength to the argument that public scrutiny was the best way to produce strong encryption and strong ciphers. What it really did, however, was to underscore an argument that had been made by the independent cryptographic community for years: secret systems were more vulnerable than public ones, because they were not as thoroughly tested, and weaknesses not immediately made public and fixed. The second Netscape hack, in particular, undermined the NSA's long-standing position that its ciphers (Skipjack, for example) had to be kept secret.

*Cracking DES*

As a lark, or rather as a demonstration to prove the ineffectiveness of the government's export regulations, the Electronic Frontier Foundation funded a project by John Gilmore and Paul Kocher to build a DES cracking machine. DES, of course, was still highly restricted. At a 1998 cryptography conference, Gilmore and Kocher used the $210,000 machine to produce the plaintext of a DES encrypted message in 24 hours. The implications of this cracking effort were obvious. If it could be done with a single unit produced for $210,000, mass production of the units would drop the price dramatically. And if the price dropped, it meant that such units were well within reach of governments, corporations, spies, criminal organizations, and anyone else who might have an incentive to want to eavesdrop. (Of course, one had to assume that the NSA already had plenty of similar units.)[242] Thus even the highly restricted DES, which the NSA had internally begun to argue was too strong for widespread use, was actually too weak to secure the nation's communications. The hackers were demonstrating, repeatedly, just how little national security benefit export restrictions provided to the government—and the government was unable to refute either their attacks or prove that the impact on the software industry and civil liberties was similarly negligible. These highly publicized hacks would be exploited by lobbyists and the software

[240] Jonathan Gornall. "Netscape Plugs Latest Leak," *The Times*, September 27, 1995, on Lexis-Nexis.
[241] For discussion of both Netscape hack efforts, see Levy, *Crypto* 278-283.
[242] Levy, *Crypto* 302.

industry to help push previously indifferent Congressmen toward liberalization of export controls on purely pragmatic terms, if not for civil liberties reasons.

### *The Software Industry Goes to Washington*

One particularly interesting result of the development of a wealthier and more politically savvy software industry was Ray Ozzie's attempt to turn the NSA against the rest of the government by appealing to its selfish organizational interests. It was a classic divide-and-conquer strategy. Ozzie came up with his own version of key escrow: one designed to appeal to the NSA, and no other branch of government, so that the NSA's interests would diverge from that of the Clinton administration and even its law enforcement allies.

The two Netscape cracks had started to make overseas buyers (those subject to the weak 40-bit keys) nervous. They wanted to know why they were saddled with weak encryption in programs like Microsoft Office and Lotus' Notes program when U.S. customers had far stronger encryption. In 1995 Ozzie came up with an ingenious solution. Ozzie was a pragmatist. While he hated crypto regulations, his decades of experience in the software industry had also shown him that waiting around for the NSA to change its mind was futile. Instead, he came up with a temporary fix. Lotus would still make two versions of Lotus notes, both with 64-bit encryption, but one would have a gift for the NSA: 24 bits of the 64 bit key would be encrypted with NSA's public key, so that only the NSA could decrypt that portion of the message. It would be called the National Security Access Field (NSAF). Thus for the NSA, the 64-bit encryption really only amounted to 40 bits, while for everyone else it would still be a 64-bit hack. Lotus filed for two patents on the scheme in December 1995, and included the innovation in its new version of Notes, Notes Release 4.

Ozzie's new scheme was a variant of key escrow, but the motivation behind it was pure genius. Ray Ozzie had not sold out, despite the worries of some who attended Ozzie's speech outlining the scheme at the January 1996 RSA Data Security Conference. Rather, he had come up with the scheme as a way of not only appeasing international customers (or at least those who didn't realize the full implications of the scheme), but more importantly, of using the NSA's own pathologies against it, in a plot to turn the NSA and the rest of the government against each other. Since Al Gore's letter to Cantwell that sounded the retreat from government controlled key escrow, the NSA had disagreed with most of the Clinton administration's encryption control ideas, including the private-facility key escrow. Private facility key escrow meant that the government would need a warrant to get a hold of the keys, but the NSA, by habit and inclination, operated in secret. It was also, despite past actions, banned from domestic surveillance.[243] Ozzie hoped that this approach would cause the NSA (and presumably its allies in the CIA/ FBI/ NIST/ DOJ) arguing against the White House, so that in the confusion, industry could sneak its own solution through.[244]

The government had other plans. On December 30, 1996, a year after the scheme was revealed, it slapped a secrecy order on Ozzie and co-inventor Charles Kaufman's patent application. The secrecy order stated that disclosing the subject matter of the patent without authorization would subject Ozzie and Kaufman as well as Lotus to penalties, including jail time.[245] The letter further instructed that all copies of the subject matter should be destroyed. Of course, there were a few minor problems with compliance. For starters, Ozzie had already spoken publicly about the scheme in detail numerous times. Second, there were about six million copies of Lotus Notes floating around, about half of them outside the U.S., which meant he and his bosses at Lotus were faced with a situation where one of the most popular software programs in the world had been deemed a government secret. Ozzie had a friend call the deputy director of the NSA, Bill Crowell, who – in what was becoming a pattern with the NSA – after a few days deemed the order a mistake and had it rescinded.

***International Cooperation and Lobbying***

The efforts of the Clinton administration in limiting encryption were not limited to domestic regulations. The national security-law enforcement lobby that held it captive pushed for international efforts as well, since the export controls were ostensibly directed at controlling access to encryption in other countries. The Clinton administration quietly sent its representatives to lobby for tighter controls in other countries, but met with little success outside of its traditional allies, Australia and Britain. Australia issued a statement to the effect that the biggest current threats to telecommunications interception were digital telephony and encryption, and Britain began to sponsor research on public-key escrow systems at the Cryptologic Research Unit of the University of London and work on a legal framework that would effectively outlaw non-escrowed encryption. The latter effort in Britain never took effect.

The Clinton administration next approached the Organization for Economic Cooperation and Development (OECD), sending representatives drawn from the national security and law enforcement communities (DOJ's Computer Crime Unit, the NSA's Stewart Baker, and the NSC were all

[243] See Tom Huston, Attachment to memo, p. 2, in United States, Senate Committee to Study Governmental Operations with respect to Intelligence Activities, ***Intelligence Activities and the Rights of Americans, Final Report, Book II***, Report 94-755, 94th Cong., 2nd Sess., April 23, 1976, 194, cited in Diffie and Landau 146, for discussion of Nixon's illegal use of the NSA to monitor communications of U.S. citizens using international facilities.

[244] For account of Ozzie's motivations and plan, see Levy, "Wisecrackers," *Wired*, April 1996, and Levy, *Crypto* 284-6.

[245] Technically, it was now IBM and not Lotus; IBM had bought Lotus a few years earlier.

represented).[246] With an organizational mission of fostering trade and development among its member industrialized democracies, the topic of encryption seemed a natural fit. The OECD already had policy guidelines for trans-border data flows (1980) and information security (1992), so in 1996, the OECD began discussing encryption. It was an unmitigated disaster for the Clinton administration. The administration's intent in sending delegates was to get an international stamp of approval on key escrow and international agreement to limit encryption. Instead, the OECD issued cryptography guidelines that actually listed one of its aims as ""*promoting* the use of cryptography [emphasis added]".[247] The guidelines further stated that "market forces should serve to build trust in reliable systems," a blow to the secret Skipjack algorithm. The OECD also recommended development of cryptographic systems be developed in response to the needs of "individuals, businesses, and [lastly] governments," with the "development and provision of cryptographic methods" determined in an "open and competitive environment". It urged that development of "international technical standards, criteria and protocols for cryptographic methods... be market driven."[248] The U.S. was in the minority on this issue. The Scandinavian countries and The Netherlands all argued for no limits on citizens' rights to use encryption, including strong cryptography without trap doors.[249] Despite all of the Clinton administration's efforts, key escrow was barely even mentioned, much less written into the guidelines.

The European Commission, another target, issued a policy paper a few months later noting that key escrow schemes were easily circumvented and that the involvement of third parties would increase the likelihood of the message being intercepted and decrypted. It also noted the difficulty of key escrow across borders, arguing that key escrow should be limited only to what was "absolutely necessary."[250]

Having been rebuffed by the OECD, European Commission (EC), and individual countries, the Clinton administration sought to use the Wassenaar Arrangement (Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, CoCom's successor) as its favored framework for limiting encryption internationally.[251] The Wassenaar members had placed encryption items on the original Dual-Use Control List, but had not determined a ceiling on the strength

[246] Diffie and Landau 220-1.

[247] *Guidelines for Cryptography Policy,* www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm, cited in Staci Levin, "Who are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls?" *Law and Policy in International Business,* Vol. 30, No. 529, Spring 1999.

[248] OECD, "Cryptography Policy Guidelines," March 27, 1997.

[249] Information Technology Security Council, Ministry of Research and Information Technology (Denmark), "The Right to Encryption," June 11, 1996; Marc Rotenberg, "U.S. Lobbies OECD to Adopt Key Escrow," *The International Privacy Bulletin,* Vol. 4, No. 2, Spring 1996, pp. 4-7; private conversation between Landau and Deborah Hurley, April 3, 1977; all cited in Diffie and Landau 221.

[250] European Commission, *Towards a European Framework for Digital Signatures and Encryption,* 1997.

[251] Stewart A. Baker & Paul R. Hurst, The Limits of Trust: Cryptography, Governments, and Electronic Commerce 605 (1998), 23-24, cited in Karim K. Shehadeh, "The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests," *American University International Law Review,* Vol. 15, No. 271, on Lexis.

of exportable encryption products and did not control those generally available or in the public domain. Hence U.S. policies were considerably more restrictive than the Wassenaar arrangement called for. In December 1998, the Clinton administration successfully lobbied for revision of the Dual-Use Control list to include a maximum 64-bit key length on exportable mass-market encryption software, hoping to curtail the competitive advantage that foreign manufacturers had over U.S. firms.[252] However, this change was largely illusory, as the Wassenaar Arrangement is a non-binding regime.[253] The U.S. policies on encryption restriction were the strictest among industrialized democracies at the time.[254] The other members of the Wassenaar Arrangement had little to lose by not complying with the regime, and much to gain. The Germans, for example, had companies taking advantage of the restrictions on U.S. companies, and were doing a brisk business selling strong cryptography around the world. The German government had little interest in restricting these sales.[255] U.S. export controls were by 1998 nearly completely useless, preventing almost no one except the average international computer user from obtaining strong encryption, which offered almost no security benefits. In game theory terms, it was a prisoner's dilemma with many players, producing an incentive to free-ride and benefit from one's own defection and others' cooperation.[256] The defectors could reasonably argue that their defection alone had little impact on the success of the regime: studies showed that in 1998, 29 other countries produced 656 encryption products as strong or stronger than U.S. sold abroad.[257] Some of these were even operating in cooperation with U.S. firms, such as joint product development partnerships formed by RSA with China and Japan, with the approval of the Dept. of Commerce.[258] In short, despite a vigorous and broad-based attempt to forward their organizational interests on the international front, the coalition of national security and law enforcement agencies failed to achieve their objectives.

[252] McNulty, see n54 – references www.wassenaar.org/list/cat5p2.pdf

[253] Shehadeh.

[254] EPIC, "Cryptography and Liberty: An International Survey of Encryption Policy", Washington, DC. 1999.

[255] Edmund Andrews, "U.S. Restrictions on Exports Aid German Software Maker," *New York Times,* April 7, 1997, D1.

[256] Kenneth A. Dursht, "From Containment to Cooperation: Collective Action and the Wassenaar Arrangement," *Cardozo Law Review,* December 1997.

[257] See Network Associates Products, Total Network Security: Cryptographic Products (visited Feb. 22, 1999) <http://www.nai.com/products/security/tis<uscore>research/crypto/crypt<uscore>surv.asp>, cited in F. Lynn McNulty, "Encryption's Importance to Economic and Infrastructure Security," *Duke Journal of Comparative and International Law,* Spring 1999

[258] "RSA Data Security, Inc. and People's Republic of China Sign MOU on Encryption Technology and Joint Research," RSA Press Release, February 2, 1996, cited in Barth and Smith, 294. See also Wendy Grossman, "Encryption Proves a Slithery Beast to Control: American Policy on the Export of Strong Ciphers is Starting to Leak Like a Sieve," *Daily Telegraph,* January 21, 1999, cited in Levin (note 47).

### *The Beginning of Liberalization: Congress Gets Involved*

*Congress, Part I: Early 1990s*

By the mid-1990s, the tides were turning, and the beginning of the end was in sight. Government attempts to control encryption relied on two legs – key escrow (Clipper) and export controls – and the first one was a failure. The second one, though it had held (with dubious impact on the international availability of strong cryptography), was crumbling, despite the NSA's best efforts to prop it up. Ongoing negotiations between Lotus' Ray Ozzie and Microsoft's Nathan Myrhvold, working with a group called the Software Publisher's Association, and the NSA, had finally resulted in a temporary compromise solution to the export control problem. The companies received an agreement for "expedited consideration" for export of shrink-wrapped retail software containing the (weaker) RC-2 or RC-4 ciphers (not DES), limited to 40-bit keys. This limit would be raised in future years to keep pace with faster computers. In exchange, the NSA would not have to write down the agreement, and the cipher had to be kept secret.[259] Neither side was happy, though. To the software industry, preventing U.S. firms from selling products that contained algorithms that were openly published everywhere from Russia to Germany was simply illogical behavior. It resulted in the suboptimal solutions of producing two versions of Notes, or giving everyone weak encryption. To the NSA, however, it was a matter of buying time. Every obstacle they could put up would slow down deployment of universal strong crypto, even if they couldn't eliminate it completely.

Still, encryption was rapidly becoming integrated into everyday life. It was becoming harder and harder to convince people that encryption was not necessary, or that it was a threat to national security. The millions of users of Lotus Notes (along with the PGP crowd) were already well aware of its benefits. Cell phone users were beginning to wonder why their communications couldn't be encrypted, since any eavesdropper with a hundred dollar scanner from Radio Shack could hear all of their conversations.[260] Even the NFL had taken to encrypting communications between its coaches on the sidelines and its players on the field so the other team couldn't listen in to figure out the next play. For an agency not used to answering questions at all, the NSA was now being forced to answer some very tough ones.[261]

Congress had finally gotten back into the game. At the instigation of the new House Representative Maria Cantwell from eastern Seattle, a region that included a bevy of high tech companies including Microsoft and Nintendo, and Sam Gejdenson, Chairman of the House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade, and Environment, hearings were held to draw

[259] Levy, *Crypto* 262.

[260] A notable example of how embarrassing eavesdropping could be was when the Prince of Wales had his cell phone calls to his mistress intercepted. See Peter Lewis, "Of Privacy and Security: The Clipper Chip Debate," *The New York Times,* April 24, 1994.

[261] Levy, *Crypto* 205.

attention to the problems with export control policies on encryption. Attempts to approach the White House, then mired in the Clipper initiative, had been rebuffed. As Gejdenson stated, "This hearing is about the well-intentioned attempts of the National Security Agency to controls that which is uncontrollable."[262] He continued, noting that the NSA "is attempting to put the genie back into the bottle. It won't happen, and a vibrant and productive sector of American industry may be sacrificed in the process."[263] While most of Congress still accepted the NSA's views, the gap between the NSA's platform and reality was becoming more and more obvious to Congress, a fact Cantwell pointed out in her opening statement, "We are here to discuss, really, competing visions of the future."

Witnesses at the hearing began pointing out the contradictions in U.S. export policy. Ray Ozzie had rigged a screen connected to his computer in Massachusetts, and demonstrated how he could download an encryption program using DES from Germany. He then pointed out that if he were to send the same software back to Germany, he would be violating federal export control laws. Steve Walker, a former NSA official now working in the corporate world, presented the results of a Software Publishers Association study showing that 264 encryption products, 123 of which used DES, were available overseas to anyone with the cash to buy them. Similar products produced by American companies, however, could not be sold because the NSA banned their export. He went on to cite examples of American companies that had lost half their European customers because it could not sell them strong cryptography, but its foreign competitors could.[264] More testimony from various members of the software and cryptography community followed in this vein. They seemed to convince the members of the committee. As Dana Rohrbacher (R-California) noted, five years earlier, he would have scolded the witnesses for seeking profit at the expense of national security. But now, "the Cold War is over. It is time for us to get on."[265]

Cantwell began preparing a bill (HR 3627, "Legislation to Amend the Export Administration Act of 1979") to fix the broken export control regime, at least with respect to encryption. It would move the decision making process out of State to Commerce, thereby avoiding the NSA review, and make shrink-wrapped, mass-market, public domain software exempt from export regulations. The Clinton administration fought back. Al Gore called Cantwell personally and told her to stop the bill. She refused, and asked them not to fight the bill but to let it run its course in Congress. The other committee members tried to get her to stop. Still, HR 3627 was introduced on November 24, 1993, and Cantwell continued her lobbying efforts, even bringing in Bill Gates to testify before the House Intelligence Committee, where he

[262] *Ibid.* 263.

[263] John Schwartz, "Bill Would Ease Curbs on Encoding Software Exports," *The Washington Post*, November 23, 1993, C1.

[264] See text of United States House of Representatives, Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software*, Hearings, October 12, 1993, 103rd Congress, First Session, cited in Levy, *Crypto* 265.

[265] Levy, *Crypto* 264, see text of testimony.

cut off a lecture on the importance of export controls and informed the committee members that the rules were nonsense.[266]

Two days before the vote, Gore's people called to make a deal. In exchange for dropping the bill, the administration would change its position. Instead of the Clipper Chip, a different voluntary escrow scheme would be offered, perhaps with more flexible software implementation, thereby avoiding the time-lag problems with the chip. Perhaps escrow facilities could even be controlled by the private sector (banks, security companies) rather than the government.[267] Cantwell discussed the proposal with the industry group Business Software Alliance, and they agreed that she should get the promises in writing. The afternoon before the vote, the letter from Al Gore arrived.

The contents of the letter were printed on the front page of the *Washington Post* the next day, when the vote had been scheduled to occur. Then the issue really blew up. As it turns out, the White House had been intended to "placate Rep. Cantwell and avoid a national debate."[268] It had exactly the opposite effect. As it turns out, the White House had neglected to consult the NSA or the FBI. Gore's people called asking to rescind the letter, but with the contents already out in public, Cantwell refused. The deal stood. The bill was dropped, the Clinton administration began backpedaling on Clipper, and no key escrow solution ever was worked out. The Clipper Chip would reappear several times during the 1990s, in various versions, but the fundamental problems with the escrow scheme – industry's opposition, the privacy issues, the lack of appeal to foreign customers and governments (to which the Clinton administration could not guarantee equal access to keys) – would never be resolved.

Three years later, spurred by the software industry's constant complaints that export control laws were causing American industry to lose business to foreign firms selling identical products, Congress got moving again. As public awareness of the need for encryption grew, the highly publicized attacks by cypherpunks on export strength encryption illustrated, and even the interception of unencrypted cell phone calls by the House Republican leadership showed, restricting encryption on national security grounds had its costs. The U.S. lacked a strong security policy for its digital infrastructure, a problem that would become more and more pressing as the internet and digital technologies became more integrated in daily life. The economic losses and civil liberties values at stake during the encryption debate had come to the forefront, overshadowing the now miniscule national security benefits of the restrictive encryption policies.

[266] *Ibid.* 266.
[267] See Paul Andrews, "U.S. Backing Away from the Clipper Chip? – Letter to Cantwell Signals Shift on Issue of High-Tech Snooping," *The Seattle Times,* July 21, 1994, A2, for description of contents of letter; see also John Markoff, "Gore Shifts Stance on Chip Code," *New York Times,* July 21, 1994, D1.
[268] Levy, *Crypto* 267.

As a concession to industry, some adjustments and liberalization in export controls were enacted. For example, on February 16, 1996, the Clinton administration finally amended a glaring omission in the export laws by inserting the "laptop exception" into ITAR. Prior to the amendment, the law prohibited individuals from carrying even very modest levels of encryption outside the country on one's laptop computer or cell phone, requiring a munitions license of the same kind required to export a tank or fighter jet to do so.[269] On November 15, 1996, President Clinton issued an Executive Order that transferred jurisdiction for encryption products, including some mass-market products, listed as defense articles to the Department of Commerce.[270] This Executive Order excluded items that the Export Administration Act already excluded from restriction on the basis that they were widely available outside the United States.[271] The executive order also shortened approval times for software employing RC-2 and RC-4, RSA algorithms that used 40-bit keys (RC-2 was the cipher used in Lotus Notes) and approved 56-bit encryption if it utilized key recovery technology. The order also set up a specific process for export controls of encryption, an official process that up until then had been lacking.

*Congress, Part 2: mid- to late-1990s*

Congress had come a long way in the five years since Maria Cantwell's ill-fated effort to change national encryption policy. More importantly, the software industry had finally learned how to play the Washington game. The software industry, now even wealthier and more powerful than ever after the tech boom of the early 1990s, had discovered how useful Washington lobbyists could be. They organized into an industry lobby called the Americans for Computer Privacy (the "Americans" had names like Microsoft, RSA, IBM, Sun, and Novell), which joined with the Business Software Alliance and civil liberties groups included the Electronic Privacy Information Center (EPIC, which engaged in a series of FOIA litigation

[269] Amendment to the International Traffic in Arms Regulations, 61 Fed. Reg. 6111 (February 16, 1996), in Barth and Smith, 292.

[270] See 22 C.F.R. sec. 121.1 (1995) (categorizing encryption products under Category XIII to the Munitions List); See Exec. Order No. 13,026, 61 Fed. Reg. 58,767-68 (1996), reprinted in 50 App. U.S.C. sec. 2403 (1999), determining that the export of encryption products could harm national security interests even where similar products are freely available from non-United States sources. See also 15 C.F.R. sec. 744, Supp. No. 1 (1999), stating that encryption hardware and software are controlled by the DOC under CCL categories 5A002, 5D002, respectively. See 15 C.F.R. sec. 742(a) (1997), defining mass-market encryption products as those that are publicly available from retailers, whether by over-the-counter, mail, or telephone transactions, that are user-friendly and do not require substantial technical support, including encryption for confidentiality purposes. See 61 Fed. Reg. 68,581 (1996) (interim rule adopted as of Dec. 30, 1996) (amending sec. 742.15(b)(1) of the Export Administration Regulations to include 40-bit mass-market encryption software among the items transferred from the United States Munitions List to the CCL), all in Shehadeh.

[271] See 50 U.S.C. app. sec. 2403(c) (1999). This section states: "The President shall not impose export controls for foreign policy or national security purposes on the export from the United States of goods or technology which he determines are available without restriction from sources outside the United States in sufficient quantities and comparable to those produced in the United States... unless the President determines that adequate evidence has been presented to him demonstrating that the absence of such controls would prove detrimental to the foreign policy or national security of the United States," in Shahadeh.

to shake loose documentation), the Electronic Frontier Foundation, and Center for Democracy and Technology. They met frequently with administration officials, and identified legislators who would help them not only promote legislative reform, but would continue to force the issue into the spotlight, to force the NSA and its agency allies into the public eye where they did not want to be, to create pressure for reform. Notable figures in the fight were a conservative Republican from Virginia, Robert Goodlatte, and a new-economy Democrat from Silicon Valley, Zoe Lofgren. They were joined in the Senate by the unlikely crypto cowboy Conrad Burns, Patrick Leahy, and Patty Murray ("the senator from Microsoft").[272] The crypto lobby also developed a new strategy, tailoring their arguments to satisfy each congressperson's particular interests, whether national security, economic growth, civil liberties, or otherwise. Many, perhaps even most, of the Congressmen who eventually came to favor liberalization were swayed by simply by the argument that the export controls and regulations did not serve their original purpose of preventing foreign access to cryptography anymore, a fact the lobbyists were quick to point out.

The new crypto lobby had taken a page from NSA's book, preparing its own version of the NSA briefings that turned NSA's national security argument on it head. Instead of warning of the need to monitor terrorists' communications, the briefings warned of the dangers terrorists could pose to the nation's own domestic digital infrastructure, which was vulnerable in part because we had failed to adopt strong cryptography to protect it. The timing was perfect. The mid-1990s marked the heyday of not only the rise of the Internet but the rise of Internet hacking – every stolen credit card number, every corrupted website, every stolen identity was another warning of a 'digital Pearl Harbor'. Even the military got into the act, beginning public discussions on "information security" and "information warfare." The hacking of the FBI website put the exclamation point on the issue. The fear that hackers, terrorists, criminals, and hostile nations would attack the U.S. through its unprotected computer system, shutting down electrical grids, weapons systems, air traffic control, and other vital computer-controlled aspects of society loomed large. The only defense, argued the new crypto lobby, was the very thing the government had been trying to suppress for a half a century: strong cryptography.

In March 1996, Sen. Patrick Leahy (D-Vermont) introduced the Encrypted Communications Privacy Act of 1996 (S. 1587), a compromise bill that relaxed export controls, affirmed the right to unrestricted domestic use of encryption, created a legal framework for key escrow and criminalized the use of encryption in furtherance of a crime.[273] A month later, Senator Conrad Burns (R-Montana) introduced the Promotion of Commerce On-Line in the Digital Era (PRO-CODE) bill, which specifically

[272] Levy, *Crypto* 304.

[273] Since his participation in this legislation, Leahy has built and cultivated a reputation as being the most Internet-friendly Senator.

prohibited mandatory key escrow, while also affirming the right to sell and use any encryption domestically, and liberalizing export controls. (S. 1726)[274] The bill, however, as Fenno and other political scientists might have predicted, got bottled up in committee, possibly trapped by legislators heavily influenced by the NSA's briefings, and probably because it was an election year and therefore unsuitable for debate of complex legislation. Burns would re-introduce PRO-CODE in 1997. (S. 377)

In 1997, Rep. Bob Goodlatte would introduce the Security and Freedom through Encryption (SAFE) Act (HR 695). As with PRO-CODE, the bill affirmed the right to buy, sell and use any encryption domestically, and forbade mandatory key escrow. It shifted export control authority for encryption to the Dept. of Commerce, and permitted export of strong encryption if similar product were overseas. The only difference between the bills was that SAFE criminalized the use of encryption to commit a crime, whereas PRO-CODE did not discuss the issue.

The pro-encryption bills, however, were threatened in both houses during the amendment process, in keeping with the predictions of theorists of the legislative process. In the Senate, the introduction of another piece of legislation sidetracked the PRO-CODE bill in the Commerce Committee. Sen. Bob Kerrey and John McCain introduced an alternative bill, replacing PRO-CODE, called the Secure Public Networks Act (S. 909). This piece of legislation denied the services of any government-sponsored certificate authorities (agencies that distributed and authenticated public keys, a critical component of any public-key based infrastructure) to those using un-escrowed cryptography.[275] In the House, even though the SAFE bill had made it out of the House International Relations committee and Judiciary committees relatively intact, in the House National Security Committee, Rep. Porter Goss and Norman Dicks had introduced an "amendment in the nature of a substitute" that completely reversed the intent of SAFE, tightening controls on export and proposing legal controls on the use of cryptography.[276]

Both bills were stuck in their respective houses until their sessions ended, ping-ponging between various committees that would amend and un-amend and re-amend the bills, going nowhere. Not until the next 106th Congress started back up in 1999 would SAFE (now HR 850), pick up again, this time with 258 co-sponsors. In the Senate, McCain had a change of heart in 1999, and completely reversed his stance on encryption.[277] S. 909 was replaced with S. 798, a "bill to *promote* electronic commerce by encouraging and facilitating the use of encryption in interstate commerce consistent with the protection of national

[274] S. 1726. 104th Congress, 2nd Session.

[275] S. 909, 105th Congress, 2nd session.

[276] Diffie and Landau 223.

[277] McCain may also have had his upcoming presidential bid in mind as a motivator for this change to the more politically popular position.

security, and for other purposes" [emphasis added].[278] McCain, once one of the loudest opponents of the SAFE Bill, was now a vocal supporter.

Although the White House was sure that Congress would never actually pass a bill liberalizing export controls, since the issue was so complicated, the stakes (national security, 1st and 5th Amendment, privacy) so high, and the risk of a Presidential veto looming, it was distressed that subcommittee and committee votes had kept the issue alive for so long. The issue, for the Clinton administration, had become a choice between the Scylla and Charybdis of encryption. If they allowed cryptography exports, terrorists might get a hold of them, and *people might die.* If they didn't allow cryptography exports, terrorists might attack the domestic infrastructure, and... *people might die.* "As one White House policy maker later explained, it came down to *how* they would die: 'Do you want them shot out of the sky with a surface-to-air missile, or do you want the floodgates on the Grand Coulee Dam to be rewired?'" For the Clinton administration, it seemed senseless to fight an uphill battle – especially since they would blamed no matter what happened.[279]

On September 16, 1998, Vice President Gore announced additional revisions to the Administration policy on encryption. First, it made permission to export 56-bit products permanent pending a one-time review by the Bureau of Export Administration, eliminating the key recovery clause. Second, it permitted the export of encryption products with limitless encryption capabilities to a number of industries, including banking and financial institutions (expansion to include worldwide subsidiaries of U.S. firms), insurance companies, health and medical organizations in all countries (not including biochemical and pharmaceutical manufacturers), except those subject to U.S. embargoes. Third, the new policy expanded export opportunities by granting license exceptions for exports to entities falling in the above categories after a one-time technical review.[280]

A year later, in September 1999, Al Gore announced a new set of regulations to be revealed in December. The regulations would include permission to export consumer-directed cryptography in any key length – a complete 180 in the administration's policy. The government had lost. The crypto lobby, with its oddball assortment of software industry behemoths, civil liberties activists, academics, geeks and paranoiacs, had beaten the NSA and its alphabet soup of law enforcement allies.

[278] S. 798, 106th Congress, 1st session.

[279] Account and quote taken from Levy, *Crypto* 305-6.

[280] Albert Gore, News Briefing on Encryption (Sept. 16, 1998); 15 C.F.R. sec. 742.15(b)(3) (1999), in Shahadeh.

## Chapter 4

*Conclusions*

The evolution of national encryption policy over the past quarter century can be interpreted as reflecting the shift in prioritization of values away from national security and toward economic growth and civil liberties during the 1990s. It can also be taken as an illustration of the difficulties of adapting national policy to keep up with rapidly changing technologies and a shifting external economic and political environment. As political scientists such as Fenno, Shepsle and Weingast theories suggest, the government's structure is designed to prevent rapid changes national policy in order to maintain stability, and in this case, the innate resistance to change was exacerbated by the NSA's successful capture of key Congressional committees and the presidency. This stability that structural resistance to change provides, however, also delays recognition of situations in which policies have ceased to be effective and slows the process of adjusting the policies to align with external conditions.

The case as a whole suggests that policy adaptation is possible but that time lags may be inevitable. Several factors contributed to the ultimate liberalization of encryption policy: a sense of crisis fueled by media attention; concentrated industry opposition to policies and/or grass roots activism; existence of policymakers without entrenched interests in an issue; and changes in the external economic, political and technological environment that shifted policymakers' value structures.

First, the spread of information played a major role in effecting policy reform. Given the NSA's capture of the executive branch and the mixed opinions of the judiciary, the only option left for those who wished to pursue policy reform was Congress, and specifically those members of Congress who had no pre-existing interests or biases in the issue. In order to convince them of the need for policy reform, however, the reformers needed to first make them aware of the existing policies and the uneven tradeoff between the small national security benefits and large economic and civil liberties costs of the policies. They needed to point out the changes in underlying technology and the external political and economic environments for those legislators that in all likelihood had not been aware of the issue until then, because the legislation had been created before they arrived or because the legislation was outside their area of expertise. To that end, the sense of crisis created by the media and the lobbying efforts of industry and civil liberties groups were critical, because they ensured not only awareness of the issue but a continual pressure to act upon that information.

As political science and organization theories suggest, crisis did spark change and adaptation to deal with the new situation in a way that would, paraphrasing Wilson, eliminate the threat to the organization's survival. That does not, however, mean that the changes effected would be optimal for the country as a whole or even produce a change in an atavistic policy; it only means that a change that would reduce pressure on the organization would be made. The NSA, faced with the prospect of widespread use of strong encryption, did adapt: it came up with the idea of key escrow, a shift from a 'no encryption' or 'no strong encryption' stance to a 'conditional encryption' stance. It was not an earth-shattering change, but it represented adaptation of a sort – and one which arguably intruded on more civil liberties than the existing policy. Congress, too, responded to earlier crises that threatened its authority: when the NSA tried to overstep its bounds and target American citizens, when it tried to circumvent the intent of the Computer Security Act, and when it pushed the Reagan administration into issuing the Poindexter Directive, Congress responded by launching investigations into the NSA and executive branch's actions. It did not change policy; it defended its bureaucratic turf and authority from the encroachment of the executive branch. Even the Clinton administration's 'adaptations' in response to public criticism of its encryption policies prior to 1999 amounted to little more than trying to alleviate pressure, rather than effect major change that would bring policy in sync with the external environment. Thus depending on crises of the 'threat to organizational survival' variety will not bring about major policy reform, only as little change as possible to deflect pressure.

Second, lobbyists, and especially concentrated corporate interests, also play a key role in the reform process because they can provide continual pressure to push the various policymaking organizations into large-scale changes when a series of small changes is not enough. Because of the difficulties of navigating the policy-making process, a lobbying group with ample funds and incentive is necessary. Populist appeal such as the civil liberties arguments also help sell the new policy, both in terms of popular appeal and providing a more politically correct rationale for changing policy – or, at minimum, rejecting the current one. This case suggests that both Stigler and Olson were correct in noting that corporate (concentrated) interests could have significant impact on the policy making, Stigler in the effects of lock-in of regulation, and Olson both for the ability of the regulated firm (agency, in this case) or another industry with a concentrated interest to impact the regulations. The danger, however, is that once the 'new' industry successfully lobbies to have its favored policies implemented, it runs the danger of then become a new captor. That is, it may well be a case of substituting one entrenched interest (the NSA) for another (the software industry), such that a few years down the road, it will be the free-export policy that is no longer in sync with environmental conditions.[281]

Third, the case also suggests the existence of an unaffiliated, unbiased segment of the policymaking elite is needed to enact broad policy changes. In this particular case, it was the congressmen not in the various national security-related committees and the 'new blood', the new representatives and senators who had as yet not been indoctrinated by NSA briefings, who filled this role. Each of the Congressmen who spearheaded the reforms was not affiliated with the intelligence or foreign relations committees in their respective houses. The NSA also recognized the importance of contacting potential

[281] Some might argue that day, in the post-September 11 environment, has already come.

allies early, before they had had a chance to develop their own positions; hence they and the FBI pursued the new Clinton administration long before the new people arrived in Washington. By the time the Clinton administration took office in January 1997, they had already adopted the NSA-FBI policies, so that the software industry and civil liberties lobbies could not even get time with them to discuss alternatives. As Truman argues, access to government officials did represent influence in the policy process.

Lastly, one of the major factors in enacting policy reform was the shift in external conditions – technological, economic, and political. The technological change was the driving factor, since it was the development and release of encryption technologies both domestically and internationally by independent cryptographers and industry that made the policies ineffective. Secondarily, the growth in use of personal computers and electronic communications created and drove a market demand for encryption products that had previously not existed, which also altered the impact of the existing policies by increasing the relative weight of the economic interests and civil liberties balanced against national security in the values tradeoff. The concurrent boom in the computer and software industry in Seattle and Silicon Valley also led to the establishment of an economic, and later political, force that could and would advocate policy reform. Lastly, the end of the Cold War meant that for many policymakers, the urgency of the national security considerations behind the original policies had lessened, such that other values could rise in relative importance.

The evolution of national encryption policy thus both fits and does not fit with the predictions made by organization and political science theories. In terms of organizational culture, the NSA was able to adapt culturally in a limited way to shifting conditions without fundamentally altering its organizational mission or its ability to achieve its ultimate objectives. In terms of political science, inertia through Stiglerian capture and the 'dead hand' of bureaucracy undoubtedly existed, but reform eventually did occur. Olsonian collective action explains the ability of the software industry and civil liberties lobbies to mobilize, but cannot account for their success in the debate against an equally motivated, concentrated, and entrenched interest. What this suggests is that the theories of public policy are formulated based on the regulation of stable, mature industries, such that the theories do not account for the possibility or impact of changing technologies, growing industries, or shifting external political and economic conditions. It was not any single one of these factors – crisis, lobbies, new Congressmen or changes in the external environment – that made sweeping reform of national encryption policy possible, but the combination of all four.

*Implications*

The implications of this case for the future of public policy are generally pessimistic. First, the case suggests that the ability of policymakers to independently recognize and move to change long-standing policies that have been rendered ineffective by changing technology is limited. This may be particularly true when the long-standing policy is justified by a politically bulletproof rationale, as was the case for the 'national security' imperative in restricting encryption exports. The presence of regulatory capture and powerful entrenched interests also delays and may even prevent the policy reform process, as shown by the efforts of the NSA to foil liberalization of export controls.

Second, the case also suggests that policy makers do not always actively realize when their underlying value structures change or how those new valuation schemes affect existing regulations that were adopted based on a different ordering of fundamental values. For example, export controls were formulated at a time when national security was the primary concern of policymakers, but when the Cold War ended, the importance of economic growth and 'softer' values like the right to privacy grew in proportion to the decline in emphasis on national security. The restrictions on encryption, therefore, were seen as less valuable in the post-Cold War period because they did not serve the now-primary interest of economic growth. Although major political events such as the end of the Cold War are rare, they are also not followed by a re-evaluation of every existing policy, even though existing regulations in many areas may have been created to serve a particular set and prioritization of objectives that no longer exist. The tendency to assume all is well unless a crisis occurs or an outside group with an interest in changing the policy to suit their own needs means that policy-making becomes purely reactionary rather than pro-active, and subject to hijacking by concentrated interests. The 'squeaky wheel' method of formulating public policy thus does not seem to be optimal for creating coherent and well-tuned national policies.

Third, the case suggests that the policy making process is poorly adapted to the regulation of fast-changing industries, as the rate of technological change inevitably outpaces that of policy reform. As such, lag times, and hence periods of poorly synchronized policies and technological conditions, may be unavoidable. There does not seem to be an easy solution to this dilemma, however. The simplest solution would be to build in more flexibility for review and adaptation into the regulations to allow adaptation during implementation, since the legislative process is so cumbersome. The drawback, however, is that as with the encryption case, the administrators may implement the regulations to serve their own needs rather than tailoring and adapting them to changing external conditions. Shifting administrative responsibility to an agency without an interest in the issue to avoid such problems clearly has even more serious disadvantages, since such an agency will likely lack the expertise to competently administer the regulations. Alternatively, it may in the process of developing the necessary expertise acquire an organizational interest in a certain interpretation of the regulations. A set independent review process may alleviate some of these issues, although the slow pace of conducting independent reviews may also hinder adaptation; by the time an independent body such as the National Research Council finishes its review, its conclusions may very well be obsolete. The resolution of the problem in the encryption case depended on the lobbying efforts of a newly emergent software industry, civil liberties lobbies and media watchdogs, particularly the first, but depending upon such groups to ensure that policies and external realities match up seems almost to be leaving policy adaptation up to luck. The coalition of forces that emerged to push for encryption policy reform cannot be assumed to exist or mobilize for every potential issue of regulation of technology.

Finally, the case suggests that national security (or any critical, primary national objective) can be used as a justification for policies and even abuses that continue long after conditions under which those objectives were formed no longer exist, because the values and mindset become embedded in the organizations created to ensure the achievement of those objectives. The constant emphasis on national security during the Cold War created within the NSA a culture that set national security above all other values, to the extent where the NSA began to overstep its legal authority and disregard even fundamental Constitutional rights in forming and implementing policy. This attitude resulted in a series of questionable actions, including the surveillance of American citizens uncovered by the Church investigations in 1977; disregarding the 1978 Department of Justice findings that export controls violated the First Amendment; and downplaying the Fifth Amendment infringements that mandatory key escrow entailed. It also enhanced a sense of entitlement rooted in the NSA's pre-history during World War II that all cryptology 'belonged' to the agency, which led to the engineering of the Poindexter Directive and the memorandum that snatched jurisdiction over civilian cryptography away from the NIST in explicit violation of the letter of the Computer Security Act, among other actions. Thus the case illustrates how reasonable and timely objectives can motivate policies that take on a life of their own long after the external conditions that prompted their creation have passed.

The implications for the present, given similar priority put on the war on terrorism, are several. Again, national security has risen to the top of national priorities, and again, an unofficial state of war has been declared. These were precisely the conditions under which the NSA were formed, and under which its worst abuses occurred. Just as the NSA was formed to protect national security then, the Department of Homeland Security was established a few years ago. The debate over the Patriot Act, which arguably violates the Fourth Amendment guarantees against search and seizure and a more general right to privacy in the name of protecting national security, is perhaps the most prominent example of the new variation on tradeoffs between national security and civil liberties.[282] The two most contentious provisions of the Patriot Act, a grab bag of enhanced police and prosecution rights, both infringe on Fourth Amendment

[282] Patriot Act is Public Law 107-56, passed October 26, 2001, six weeks after September 11, 2001.

protections against search and seizure. The first provision allows authorities to search people's homes without notifying them at the time. The second grants the government authority to go through library, business, medical, and other personal records, again without prior notification. A FBI internal memorandum issued as a guideline to agents states that "tangible things" may be taken during secret searches, including apartment keys. As with the NSA, secrecy plays a large role: individuals whose records are requested are barred from revealing the request, and the FBI is not required to notify individuals that their records or homes are being searched.[283] Thus, it is difficult to determine if, when, how, or how often the Patriot Act is exercised – just as it was difficult or even impossible to determine how many patents and papers the NSA classified – which means that abuses may be difficult to uncover until it is too late. In perhaps a troubling sign, the Department of Justice in July 2004 released a report indicating that the Patriot Act, intended as anti-terrorism legislation, had already been used to expand police authority to use in other cases, including breaking pornography rings and solving kidnappings.[284] While those were undoubtedly good intentions, the troubling aspect is the implications of expanding the scope of such broadly written legislation to ordinary crimes and eventually the prevention of ordinary crimes and beyond. The potential for abuse is enormous, and secrecy limits the ability of the public to know of those abuses. Freedom of Information Act requests and litigation can only reveal so much, and the need for such requests to wind their way through bureaucracy only increases the chances that any abuses will be caught too late. As Senator Frank Church stated during the investigations of the NSA in 1975, "That capability [of eavesdropping anywhere] at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide."[285] His comments referred to the NSA, but they ring true for the worst case scenarios of the Patriot Act as well. The dominance of national security on the national agenda since September 11, 2001, has already created in American society a debate over national security versus civil liberties similar to that seen during the period of liberalization of encryption regulations. The pattern of behavior by the government suggests that another, similar debate over another regulation or industry may well occur in the future, as once again technological advances and changes in the external environment render older policies ineffective and shift their underlying values tradeoffs.

[283] Timothy Egan, "Sensing the Eyes of Big Brother, and Pushing Back," *New York Times,* August 8, 2004, A20.
[284] Daniel Eggen, "Justice Dept. Report Details Use of Patriot Act," *Washington Post,* July 14, 2001, A7. The report is: U.S. Department of Justice, "Report from the Field: The U.S. Patriot Act at Work," July 2004, available at http://www.lifeandliberty.gov/docs/071304_report_from_the_field.pdf.
[285] Bamford 4.

## *Epilogue: The Future of Encryption*

*"It may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."*

-- Edgar Allen Poe

Although cryptography dates back nearly 4000 years to Mesopotamia, the past thirty years have seen perhaps the greatest and most rapid advancements in the history of cryptology. The development of public key ciphers was the first major breakthrough. The next is probably quantum cryptology, which when fully developed, which will mark the end of the era of public key. The majority of current encryption algorithms in use rely upon large prime numbers for their strength because of the difficulty of factoring. Until a better factoring algorithm is found, or quantum computing becomes a reality, RSA and other factoring-based algorithms are safe.[286] Quantum computing reduces key cracking to the functional equivalent of encoding and decoding. That is, for a quantum computer, the physics are such that encryption, decryption, and forcible decryption are almost equally easy. With current Turing machine-type computers, breaking a key is an exponential function: every additional bit in key length multiplies the difficulty of finding that key by a factor of two, so that twice as much time, processing power, memory, or other resources are needed. Quantum computing collapses the difficulty of key-cracking from an exponential function to a polynomial function, which puts it on par with the effort needed to encode or decode (with the correct key).[287] Thus, production of a functional quantum computer renders current public key technology extremely insecure.

The current state of research into quantum computing has at least theoretically solved the problem of key distribution. That is, it has solved the original problem with one-time pads, which are the 'gold standard' in terms of cryptography: mathematically unbreakable. In the past, the distribution of the one-time pads was prohibitively expensive, which limited their use. Quantum computing can, by using the laws of physics rather than relying upon human security measures, allow the production and use of secure one-time pads without the hazards of central distribution. A few two- and three-bit quantum computers that can do some basic computation have been produced, and at least two companies have begun producing a few elements of a quantum cryptographic system.[288] However, the field is still in its pioneering stages, with issues of error correction, decoherence (decay of the computer from a quantum to

[286] As Giles Brassard, a cryptographer, stated in the first issue of RSA Security's own journal, "I think that I shall see a special-purpose quantum factorization device in my lifetime. If this happens, RSA will have to be abandoned." Giles Brassard, *Crypto Bytes,* Vol. 1, No. 1, Spring 1995.

[287] For an algorithm to be fast by computer science standards, the time it takes to execute the algorithm must increase no faster than a polynomial function of the size of the input. For a much more detailed and comprehensive discussion of the physics and computer science behind quantum computing, please see www.qubit.org, the website of Oxford University's Centre for Quantum Computation.

[288] See MagiQ Technologies' website at www.magiqtech.com

an incoherent state due to interactions with the environment), and hardware architecture remaining unsolved.[289] For cryptographic purposes, the mechanics of signing and key authentication are as yet unresolved, so a deployable quantum cryptographic system is still far in the future, despite enthusiastic research funded by the NSA and conducted at centers around the world.

Ultimately, cryptography is not a technical issue, but a human one. Poe was wrong: human ingenuity has concocted a cipher that human ingenuity cannot solve. It is called the one time pad.[290] However, the one-time pad is only *theoretically* impenetrable. As with all things, human error can negate even the security of one-time pads. One time pads depend upon generating a truly random key, and of course, on using the pads only once. A famous cryptanalysis effort during the Cold War involved the breaking of Soviet one-time pads that had accidentally been produced and used twice – the Venona decrypts. The Venona documents allowed American cryptanalysts to read not only diplomatic communications but communications about Soviet atomic bomb espionage efforts, as well as other KGB communications between various KGB and GRU (Soviet Army General Staff Intelligence Directorate) and GRU-Naval offices.[291] Thus even in the tensest of times, using the most secure system available, human error can undo all of the security that technology can provide.

Quantum cryptography, or any other cryptographic system, can provide a technical fix for the problem of secure communications, but it cannot prevent human error or human carelessness. Those determined to eavesdrop, to break into secure communications, will find a way. If and when quantum computing makes technological eavesdropping impossible, the social engineering solution to breaking a cryptosystem will remain. The two koans of cryptography hold true. First, never underestimate the amount of effort your adversary will devote to cracking your encryption. The resources governments and spy agencies around the world are devoting to quantum computing for the express purpose of making the 'functionally uncrackable' RSA and other algorithms obsolete, should be proof enough. Second, look for plaintext. The most difficult way is always a brute force attack, but sometimes human error, whether in a random number generator in Netscape or production slip-up in the Soviet Union, will provide a shortcut. Software programmers often joke that producing computer software is a race between the programmers to

[289] http://www.cs.caltech.edu/~westside/quantum-intro.html. I would like to thank Jake Taylor for explaining and the physics behind quantum computing and quantum cryptography to me. Any errors in the explanation above are, unfortunately, mine.

[290] See http://www.worldhistory.com/wiki/O/One-time-pad.htm for explanation of one-time pads. For proof of mathematical inpenetrability, see Claude Shannon. "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol.28(4), page 656–715, 1949. Available online at http://www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf.

[291] See Benson, Robert Louis. *The Venona Story* (Fort George G. Meade, Md.: National Security Agency, Center for Cryptologic History, 2001), and John Earl Haynes, *Venona: Decoding Soviet Espionage in America* (New Haven: Yale Univ. Press, 1999).

create an idiot-proof program and nature to produce a bigger idiot. The same holds true of cryptography. A human communications chain always has weak links, whether it is the typist who leaves her computer unsecured while she gets her coffee, the secretary who gets drunk at a party, the senator's aide who prints out too many copies of a classified communication, the woman who uses her daughter's name as a password, or the man who leaves his computer password on a Post-It note taped to his computer monitor. Ultimately, there is no such thing as a perfectly secure cryptosystem, because humans are the ones using the system.

## Bibliography

### *Technical aspects of cryptography*

Blaze, Matthew. "Protocol Failure in the Escrowed Encryption Standard," *Proceedings of the Second ACM Conference on Computer and Communications Security,* November 1994.

Churchmore, Robert. *Codes and Ciphers: Julius Caeser, the Enigma, and the Internet.* Cambridge: Cambridge University Press, 2002.

Feistel, Horst. "Cryptography and Computer Privacy." *Scientific American.* Vol. 228, No. 5 (May 1973), 15-23.

Gaines, Helen Fouché. *Cryptanalysis: A Study of Ciphers and their Solution.* New York: Dover Publications, 1956.

Lewand, Robert Edward. *Cryptological Mathematics.* Mathematical Association of America, 2000.

Raber, Ellen and Michael O. Riley. "Protective Coatings for Secure Integrated Circuits," *Energy and Technology Review,* May-June 1989, 13-20.

Ron Rivest, Adi Shamir, and Len Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," MIT/ Laboratory for Computer Sciences Technical Memo, No. 82, April 4, 1977.

Shannon, Claude. "Communication Theory of Secrecy Systems", *Bell System Technical Journal,* Vol. 28, No. 4, 656–715.

Sinkov, Abraham. *Elementary Cryptanalysis.* Mathematical Association of America, 1966.

### *Organization Theory*

Gagliardi, Pasquale. "The Creation and Change of Organizational Cultures: A Conceptual Framework," *Organization Studies,* Vol. 7, No. 2, 117-134.

March, James P., and Johan P. Olsen. "The New Institutionalism: Organizational Factors in Political Life," *American Political Science Review,* Vol. 78, No. 3 (Sept. 1984), 734-749.

Pettigrew, Andrew M. "On Studying Organizational Cultures," *Administrative Science Quarterly,* Vol. 24, No. 4, Qualitative Methodology (December 1979), 570-581.

Smirich, Linda. "Concepts of Culture and Organizational Analysis," *Administrative Science Quarterly,*Vol 28, No. 3, Organizational Culture (Sept. 1983), 339-358.

Schein, Edgar. "Coming to a New Awareness of Organizational Culture," *Sloan Management Review,* Vol. 25, No. 2, 3-16.

Wilson, James Q., "Innovation in Organizations: Notes Toward A Theory," in James D. Thompson, *Approaches to Organizational Design.* Pittsburgh: University of Pittsburgh Press, 1966, 194-219.

---------. *Bureaucracy: What Government Agencies Do and Why They Do It.* New York: Basic Books, 1989.

***Political Science***

Allison, *Essence of Decision: Explaining the Cuban Missile Crisis.* New York: HarperCollins, 1971

--------. "Conceptual Models and the Cuban Missile Crisis," in *American Foreign Policy: Theoretical Essays.* Ed. G. John Ikenberry. New York: Longman, 1999.

Fenno, Richard. *Congressmen in Committees.* Berkeley: Institute of Governmental Studies Press, 1995.

Finnemore, Martha. *National Interests in International Society.* Ithaca: Cornell University Press, 1996.

Kingdon, John W. *Agendas, Alternatives, and Public Policies.* Boston: Little, Brown, and Company, 1995.

Latham, Earl. *The Group Basis of Politics: A Study of Basing-Point Legislation.* New York: Octagon Books, 1965.

McCubbins, Mathew D., Roger G. Noll, and Barry R. Weingast, "Administrative Procedures as Instruments of Political Control," *Journal of Law, Economics, and Organizations,* No. 3 (1987), 243-277.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups.* Cambridge: Harvard University Press, 1965.

--------. *The Rise and Decline of Nations.* New Haven: Yale University Press, 1982.

Shepsle, Ken, and Barry Weingast, "The Institutional Foundations of Committee Power," *American Political Science Review*, Vol. 81, No. 1 (March 1987), 85-104.

Stigler, George J. "The Theory of Economic Regulation," *Bell Journal of Economics* No. 2 (1971), 2-21.

Truman, David. *The Governmental Process: Political Interests and Public Opinion.* New York: Alfred A. Knopf, 1953.

Wildavsky, Aaron. *Speaking Truth to Power: The Art and Craft of Policy Analysis.* Boston: Little, Brown and Company, 1979.

Zuckerman, Brian. "Long-Term Trends, Adaptation, and Evaluation in U.S. Regulatory Policy." Ph.D. dissertation, Massachusetts Institute of Technology, Department of Political Science, 1993.

***General***

------. "U.S. Security Aide Accused of Taking Secret Documents," *New York Times,* October 10, 1954, pg. 1.

Andrews, Edmund. "U.S. Restrictions on Exports Aid German Software Maker," *New York Times,* April 7, 1997, D1.

Andrews, Paul. "US Backing Away From the Clipper Chip? Letter to Cantwell Signals Shift on Issue of High-Tech Snooping," *Seattle Times,* July 21, 1994, A2.

Bamford, Diffie, Landau and Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," *Science,* Vol. 97, July 29, 1977, 438-40.

Bamford, James. *The Puzzle Palace.* Boston: Houghton Mifflin Co., 1982.

Barth, Richard C. and Clint N. Smith. "International Regulation of Encryption: Technology Will Drive Policy," in Brian Kahin and Charles Neeson, *Borders in Cyberspace.* Cambridge: MIT Press, 1998, 283-299.

Benson, Robert Louis. *The Venona Story.* Fort George G. Meade, Md.: National Security Agency, Center for Cryptologic History, 2001.

Beth, Th., M. Frisch and G.J. Simmons, eds., *Public Key Cryptography: State of the Art and Future Directions,* Lecture Notes in Computer Science, No. 578, Springer-Verlag.

Giles Brassard, *Crypto Bytes,* Vol. 1, No. 1, Spring 1995

Browning, John. "I Encrypt, Therefore I Am." *Wired.* November 1997.

William M. Bulkeley, "Cipher Probe: Popularity Overseas Of Encryption Code Has the U.S. Worried --- Grand Jury Ponders if Creator `Exported' the Program Through the Internet --- `Genie Is Out of the Bottle"', *The Wall Street Journal,* 28 April 1994, A1.

Burnham, David. *The Rise of the Computer State.* Random House: New York, 1980.

Chartrand, Sabra. "Clinton Gets a Wiretapping Bill that Covers New Technologies," *New York Times,* October 9, 1994, A27.

Davida, George. "The Case Against Restraints on Non-governmental Research in Cryptography," reprinted in *Cryptologia,* Vol. 5, No. 3, July 1981.

Davis, Bob. "A Supersecret Agency Finds Selling Secrecy to Others Isn't Easy," *Wall Street Journal,* March 28, 1988.

Diffie, Whitfield and Susan Landau. *Privacy on the Line.* Cambridge: MIT Press, 1997.

Egan, Timothy. "Sensing the Eyes of Big Brother, and Pushing Back," *New York Times,* August 8, 2004, A20.

Eggen, Daniel. "Justice Dept. Report Details Use of Patriot Act," *Washington Post,* July 14, 2001, A7.

Elmer-Dewitt, Philip. "Who Should Keep the Keys?", *Time,* March 14, 1994.

Garfinkel, Simson. *PGP: Pretty Good Privacy.* New York: O'Reilly & Associates, 1995.

Gornall, Jonathan. "Netscape Plugs Latest Leak," *The Times,* September 27, 1995.

Grossman, Wendy. "alt.scientology." *Wired.* December 1995.

----------. "Encryption Proves a Slithery Beast to Control: American Policy on the Export of Strong Ciphers is Starting to Leak Like a Sieve," *Daily Telegraph,* January 21, 1999.

Haynes, John Earl. *Venona: Decoding Soviet Espionage in America.* New Haven: Yale Univ. Press, 1999.

Hoffman, Lance, ed. *Building in Big Brother: The Cryptographic Policy Debate.* New York: Springer-Verlag, 1995.

Kahn, David. *The Codebreakers.* New York: MacMillan, 1967.

Kimery, Anthony. "Big Brother Wants to Look Into Your Bank Account (Any Time It Pleases)." *Wired,* December 1993.

Koops, Bert-Jaap. *The Crypto Controversy: A Key Conflict in the Information Society.* The Hague: Kluwer Law International, 1999.

Kruh, Louis. "Cryptology and the Law---VII," *Cryptologia,* Vol. 10, No. 4, October 1986.

LaMacchia, Brian and Adnrew Odlyzko. "Computation of Discrete Logarithms in Prime Fields," *Design, Codes, and Cryptography,* Vol. 1, 1991, 47-62.

Lescaze, Lee. "Pentagon vs. CIA: Control of Intelligence Community Sparks Major Institutional Battle," *Washington Post,* June 10, 1977, A1.

Leviero, Anthony. "Dutch Say Petersen Gave Data, But They Thought He Had Right," *New York Times,* October 20, 1954, p. 1.

Levy, Steven. "Crypto Rebels." *Wired.* May/June 1993.

----------.. "The Cypherpunks versus Uncle Sam." *New York Times Magazine,* June 12, 1994.

----------.. "Prophet of Privacy." *Wired.* November 1994.

----------. "E-Money. That's What I Want." *Wired.* December 1994.

----------. "Wisecrackers." *Wired.* March 1996.

----------. "Clipper Chick." *Wired.* September 1996.

----------. "The Open Secret," *Wired,* April 1999.

----------. *Crypto.* New York: Viking, 1999.

Lewis, Peter. "Of Privacy and Security: The Clipper Chip Debate," *New York Times,* April 24, 1994, C5.

Markoff, John. "Paper on Codes is Sent Despite US Objections," *New York Times,* August 9, 1989.

----------. "Flaw Discovered in Federal Plan for Wiretapping," *New York Times,* June 2, 1994, A1.

----------. "Gore Shifts Stance on Chip Code," *New York Times,* July 21, 1994, D1.

----------. “A Secret Computer Code is Out,” *New York Times*, September 17, 1994, A37.

Mintz, John. “Intelligence Community in Breach with Business,” *Washington Post*, April 30, 1992, A8.

Quittner, Joshua. “The Merry Pranksters Go to Washington.” *Wired*. June 1994.

Reinsch, William. *U.S. Dual-Use Export Controls*. United Stated Information Agency, *Economic Perspectives*, September 1997. At htpp://usinfo.org/trade/ejou997/ejreinsch.htm.

Schwartz, John. “Bill Would Ease Curbs on Encoding Software Exports,” *Washington Post*, November 23, 1993, C1.

Schwartz, John. “The Software Security ‘Threat’: US Fears Foreign Use of Encryption Features,” *Washington Post*, June 18, 1994, A1.

Shapley, Deborah. “DOD Vacillates on Wisconsin Cryptography Work,” *Science*, Vol. 201, July 14, 1978, 141.

----------. “NSA Slaps Secrecy Order on Inventors’ Communications Patent,” *Science*, Vol. 201, September 8, 1978, 891-94.

Singh, Simon. *The Code Book*. New York: Doubleday, 1999.

Tran, Mark. “Student Cracks Code on Internet Security Software,” *The Guardian*, August 18, 1995, 11.

Van Bakel, Rogier. "How Good People Helped Make a Bad Law.” *Wired*. February 1996.

Weber, Thomas E. “Should Only the Paranoid Get E-Mail Protection? --- Probably Not, As `Encryption' Gets Easier,” *The Wall Street Journal*, September 25, 1997, B6.

Weingarten, Fred. “Cryptography: Who Holds the Key?” *SIAM News*, January/February 1997.

### *Legal*

Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999).

Broadbent, R. Aylan. “US Export Controls on Dual-Use Goods and Technologies: Is the High-Tech Industry Suffering?” *Currents: International Trade Law Journal*, Vol. 8, No. 49 (Summer 1999).

Dursht, Kenneth A. “From Containment to Cooperation: Collective Action and the Wassenaar Arrangement,” *Cardozo Law Review*, Vol. 19, No. 1079 (December 1997).

Junger v. Daly, 8 F. Supp. 2d. 708 (N.D. Ohio 1998),

Karn v. United States Department of State. 925 F. Supp. 1 (D.D.C 1996).

Levin, Staci I. “Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls,” *Law and Policy in International Business*, Vol. 30, No. 529 (Spring 1999).

McNulty, F. Lynn. "Encryption's Importance to Economic and Infrastructure Security," *Duke Journal of Comparative and International Law,* Vol. 9, No. 427 (Spring 1999).

E. John Park, "Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security," *Virginia Journal of Law and Technology,* Vol. 2, No. 3 (1997).

Ross, Patrick I. "Computer Programming Language: Bernstein v. United States Department of State," *Berkeley Technological Law Journal,* Vol. 13, No. 305 (1998).

Saundersby, Kurt M. "The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff," *John Marshall Journal of Computer and Information Law,* Vol 17, No. 945 (Spring 1999).

Shehadeh, Karim K. "The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests." *American University International Law Review,* Vol. 15. No. 271.

Smith, Charles Barry. "Current US Encryption Regulations: A Federal Law Enforcement Perspective," *New York University Journal of Legislation and Public Policy,* Vol. 3, No. 11 (1999/2000).

United Nations Declaration of Human Rights, http://www.hrweb.org/legal/udhr.html.

***Primary Documents***

Computer Professionals for Social Responsibility (CPSR), David Banisar and Marc Rotenberg, eds. *1993 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls,* 1993

Kenneth Dam and Herbert Lin, eds., National Research Council, Commission on Physical Sciences, Mathematics, and Applications, Computer Science and Telecommunications Board, Committee to Study National Cryptography Policy, *Cryptography's Role in Securing the Information Society,* National Academy Press, 1996.

Electronic Privacy Information Center (EPIC), David Banisar, ed. *1994 Cryptography and Privacy Sourcebook: Primary Documents on US Encryption Policy, the Clipper Chip, the Digital telephony Proposal and Export Controls.* Diane Publishing, Upland, Pennsylvania, 1994.

European Commission, *Towards a European Framework for Digital Signatures and Encryption,* 1997

Louis Freeh, Speech to American Law Institute, May 19, 1994, in EPIC 1994, 6.

---------. Speech to the Executives' Club of Chicago, February 17, 1994

---------. Testimony in USS 103b, 5-51.

---------. Statement to Committee on Commerce, Science, and Transportation, U.S. Senate, July 25, 1996.

Tom Huston, Attachment to memo, p. 2, in United States, Senate Committee to Study Governmental Operations with respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans, Final Report, Book II,* Report 94-755, 94th Cong., 2nd Sess., April 23, 1976.

International Trade in Armaments Regulations text at http://pmdtc.org/reference.htm.

Bruce Schneier and David Banisar, eds. *The Electronic Privacy Paper.* New York: J. Wiley, 1997.

Brent Scrowcroft, Memorandum to Secretary of Defense Dick Cheney, Attorney General William Barr, and Director of Central Intellience Robert Gates, January 17, 1992

United States Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606.

United States Department of Commerce, National Institute of Standards and Technology, and United States Department of Defense, National Security Agency, "Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency concerning the Implementation of Public Law 100-235," March 24, 1989.

United States Department of Commerce, National Institute of Standards and Technology, "Memorandum for the Record, January 31, 1990."

United States Department of Commerce, National Institute for Standards and Technology, "Memorandum for the Record, March 26, 1990."

United States Department of Commerce, National Institute of Standards and Technology. *Publication XX: Announcement and Specifications for a Digital Signature Standard (DSS),* August 19, 1991.

United States Department of Commerce, National Institute of Standards and Technology, "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard," *Federal Register,* Vol. 59, No. 27, February 9, 1994.

United States Department of Commerce, National Institute of Technology and Standards, "Public Key Status Report," in EPIC 1996, p. C-3.

United States Department of Justice, "Report from the Field: The U.S. Patriot Act at Work," July 2004, available at http://www.lifeandliberty.gov/docs/071304_report_from_the_field.pdf.

United States General Accounting Office, "Communications Privacy: Federal Policy and Actions," GAO/OSI-92-2-3, November 1993.

United States General Accounting Office, *Communications Privacy: Federal Policy and Actions,* Letter Report, April 8, 1997, GAO/AIMD-97-49.

USHR, Committee of Government Operations, Government Information, and Individual Rights Subcommittee, *The Government's Classification of Private Ideas,* 96th Congress, 2nd Session, 1980.

United States General Accounting Office, *Communications Privacy: Federal Policy and Actions,* (Letter Report, April 8, 1997, GAO/AIMD-97-49).

United States House of Representatives, Committee of Government Operations, Government Information, and Individual Rights Subcommittee, *The Government's Classification of Private Ideas,* 96th Congress, 2nd Session, 1980.

United States House of Representatives, Committee on Government Operations, Subcommittee, *Computer Security Act of 1987,* Hearings on HR 145, February 25, 26, and March 17, 1987, 100th Cong., 1st Sess., 1987, 381.

United States House of Representatives, Committee on Government Operations, House Report 100-153, Part 2, *Report on the Computer Security Act of 1987,* 100th Cong., 1st Sess., Washington, D.C.

United States House of Representatives, Committee of Government Operations, Legislative and National Security Subcommittee, *Military and Civilian Control of Computer Security Issues,* Hearings on May 4, 1989, 101st Cong., 1st Sess., 1989.

United States House of Representatives, Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade and Environment, *Export Controls on Mass Market Software,* Hearings, October 12, 1993, 103rd Congress, 1st Session.

United States House of Representatives, Committee on the Judiciary, *Report on Telecommunications Carrier Assistance to the Government,* HR103-827, 103rd Cong., 2nd Sess.

United States Senate, Committee on the Judiciary, Subcommittee on Technology and the Law (Senate), and United States House of Representatives, Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services,* Joint Hearings on HR 4922 and S. 2375, March 18 and August 11, 1994, 103rd Cong., 2nd Sess.