Managing Uncertainty: Foresight and Flexibility in Cryptography and Voice over IP Policy

by

Shirley K. Hung

M.S. Political Science
Massachusetts Institute of Technology, 2004

A.B. Government
Harvard University, 2000

Submitted to the Department of Political Science in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy in Political Science

at the

Massachusetts Institute of Technology

February 2008

Signature of Author: _____
Department of Political Science
January 9, 2008

Certified by: _____
Kenneth A. Oye
Associate Professor of Political Science
Thesis Supervisor

Accepted by: _____
Edward S. Steinfeld
Chairman, Graduate Program Committee

This page deliberately left blank.

Managing Uncertainty: Foresight and Flexibility in
Cryptography and Voice over IP Policy

by

Shirley K. Hung

Submitted to the Department of Political Science
in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy in
Political Science

ABSTRACT

This main question in this dissertation is under what conditions government agencies show foresight in formulating strategies for managing emerging technologies. A secondary question is when they are capable of adaptation. Conventional wisdom and most organization theory literature suggest that organizations are reactive rather than proactive, reluctant to change, and responsive only to threats to their core mission or autonomy. The technological, economic, social, political, and sometimes security uncertainties that often accompany emerging technologies further complicate decision-making. More generally, organizations must often make decisions under conditions of limited information while guarding against lock-in effects that can constrain future choices.

The two cases examined in this dissertation suggest that contrary to conventional wisdom, organizations can show foresight and flexibility in the management of emerging technologies. Key factors that promote foresight are: an organizational focus on technology, with the emerging technology in question being highly relevant to the organization's mission; technical expertise and a recognition of the limits of that knowledge; and experience dealing with other emerging technologies.

The NSA recognized the inevitability of mass market encryption early on and adopted a sophisticated strategy of weakening the strength of, reducing the use of, and slowing down the deployment of mass market encryption in order to preserve its ability to easily monitor communications. The Agency showed considerable tactical adaptation in pursuit of this goal.

The FCC adopted a rather unusual policy of forbearance toward VoIP. The Commission deliberately refrained from regulating VoIP in order to allow the technology to mature, innovation to occur, uncertainties to resolve, and to avoid potential market distortions due to too-early or suboptimally formulated regulation. Eventually, however, pressure from outside interests such as law enforcement forced the Commission to act.

Thesis Supervisor: Kenneth A. Oye
Title: Associate Professor of Political Science

This page deliberately left blank.

Acknowledgements

It is impossible to go through grad school without incurring many debts of gratitude. My first thanks goes to my committee: Ken Oye, Gene Skolnikoff, David Clark, and Roe Smith. Ken helped me navigate the minefield that is graduate school, and brought me into PoET, a group through which I have met many extraordinary people.

Gene generously agreed to serve on my committee as an emeritus professor, and I cannot imagine anyone whose knowledge and experience were better suited to the task. His comments were always helpful and insightful, even—perhaps especially—the ones I found initially vexing because I could not come up with a good way to respond to them.

Dave is not only a legend in computer science, he is one of the most unpretentious and open-minded people I have ever met. He was unfailingly generous with his time, and amazingly patient and tolerant of my lack of technical skills. His understanding of policy, too, put me to shame as a social scientist—Dave never failed to ask questions that made me wonder, "Why didn't *I* think of that?" Unfortunately, this thought was often followed by, "And why doesn't social science have an answer to that?"

Roe. I can't even type his name without smiling. Roe opened my eyes to a whole new way of seeing technology and its interaction with the world. His reading seminar, along with the many dinners and discussion we have had about history, life, or nothing at all are among my happiest memories of graduate school

I thank the National Science Foundation for the Graduate Research Fellowship, which funded my master's thesis that became the basis of this dissertation. I thank the NSF again indirectly for funding the IGERT Program on Emerging Technologies, through which I have met so many friends and mentors and been exposed to so many new and interesting ideas.

Many thanks to Frank Field and Larry McCray for their advice and support over the past several years. Frank did his best to teach this non-engineer about engineering, explaining all the basic concepts I was too embarrassed to ask anyone else. Larry did his best to keep me intellectually honest and prevent me from retreating into unthinking cynicism about Washington bureaucracies. Chintan Vaishnav, Sharon Gillett, and Bill Lehr each provided invaluable assistance in understanding telecommunications, VoIP, and especially the labyrinth that is the FCC.

Susan Twarog helped me manage all the details of the MIT bureaucracy that so often escape me, provided an always sympathetic ear for the grad student blues.

I find it simultaneously amazing and slightly disturbing that I have been at MIT long enough to meet so many wonderful people. Nonetheless, I am grateful and proud to know all of them. I have sorely neglected my friends during this maddening dissertation process, but I look forward to getting reacquainted with them all: Hanna Breetz, Kieran Downes, Brendan Green, Chris Hodge, Llewellyn Hughes, Kristen Jamison, Casey Johnson-Houlihan, Loretta Kim, Heidi Knuff, Jon Lindsay, Austin Long, Betsy Masiello, Alex Mozdzanowska, Gautam Mukunda, J.C. Nave,

Christine Ng, Anastassia Paskaleva, Josh Shifrinson, and Jeremy Streatfeild, and so many others who I do not have room to list.

Last but not least, I thank my family. My parents gave me the intellectual drive and still provide the voices in my head that keep me going. And my brother, Alex, always made sure I kept things in perspective.

Despite all the help and encouragement from all my friends above, any errors in this thesis, unfortunately, remain mine.

Table of Contents

Table of Figures

Abbreviations

AFSA	Armed Forces Security Agency
ASA	Armed Security Agency
CALEA	Communications Assistance for Law Enforcement Act
CASI	Cryptology Amateurs for Social Irresponsibility
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
CSTB	Computer Science and Telecommunications Board
CDT	Center for Democracy and Technology
DCI	Director of Central Intelligence
DES	Digital Encryption Standard
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DSS	Digital Signature Standard
EC	European Commission
EES	Escrowed Encryption Standard (Clipper Chip)
EFF	Electronic Frontier Foundation
EPA	Environmental Protection Agency
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
FWD	Free World Dialup
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
LEA	Law Enforcement Agency
LEAF	Law Enforcement Access Field
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NRC	National Research Council Also, Nuclear Regulatory Commission
NRO	National Reconnaissance Office

NSA	National Security Agency
NSC	National Security Council
NSDD	National Security Decision Directive
OCR	Optical Character Recognition
OECD	Organization for Economic Cooperation and Development
OPP	Office of Plans and Policy (in the Federal Communication Commission)
OSHA	Occupational Safety and Health Administration
OTA	Office of Technology Assessment
PGP	Pretty Good Privacy
PTT	Postal Telegraph and Telephone, or Public Telegraph and Telephone
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman. Refers to both 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
USAID	United States Agency for International Development
USCIB	United States Central Intelligence Board
USHR	United States House of Representatives
USS	United States Senate
VoIP	Voice over Internet Protocol

Chapter 1
Introduction

Question

This dissertation seeks to answer the question of when government agencies show foresight in formulating policies for managing emerging technologies. A secondary question is when they are capable of adaptation. Organizations often must deal with new technologies. Emerging technologies present a particular complicated situation because they often create not only technological uncertainty as they evolve, but also social, economic, and political uncertainties. The conventional wisdom in political science, much of it derived from organizational and bureaucratic theory, suggests that organizations are reluctant to change, and that change is usually reactive, not proactive. That is, they respond primarily only to threats to their core mission or autonomy, and adapt only when forced to by crises, failures or external pressures.

The two cases examined in this study contradict the conventional wisdom. Both the National Security Agency (NSA) and Federal Communications Commission (FCC) showed foresight in their management of mass market encryption and Voice over Internet Protocol (VoIP, or Internet telephony) technologies, respectively. In addition, the NSA showed considerable tactical adaptation in pursuit of its policy over a period of nearly twenty-five years. Both agencies looked forward and formulated flexible policies for managing emerging technologies. While there is not enough evidence to pinpoint a single explanation for why both organizations were able to show foresight, the cases suggest several factors. First, technology played a central role in both organizations' missions, which created an incentive to not only be aware of but to anticipate emerging technologies. Second, both organizations had a long history of managing emerging technologies, which had taught them the need to build flexibility into their policies to accommodate the uncertainties that almost invariably accompany emerging technologies. Third, both organizations were expert in their technologies, and more unusually, seemed aware of the limits of their knowledge, which helped them identify the areas where greater uncertainty and policy flexibility would be needed.

Significance

It has become something of a cliché to state that technology plays an increasingly important role in our lives today, and emerging technologies ever more so. What is sometimes overlooked is the role that government agencies play in shaping which technologies emerge and their eventual form. The government's indirect role in technological innovation is widely recognized to be significant, yet is poorly understood.[1] Commercial technology is developed by businesses, and businesses are sensitive to the political and regulatory framework into which they must attempt to position and market their products. If the regulatory environment is unfavorable or hostile, whether deliberately or through benign neglect, the technology will likely not be explored or developed. Potential avenues for technological innovation may therefore be abandoned, causing society to lose out on both a new and potentially better product as well as the improvement in older products created by competition.

Proactive policies, in contrast to reactive policies, can prevent such lost opportunities for innovation because they allow for action before potential avenues for development are cut off. Reactive policies face greater temporal and political pressure, as media attention or a perceived crises is often what drives governments to act in response to new technologies, which limits options. In addition, the more developed a technology is, the more entrenched interests with a stake in the issue are likely to exist. These stakeholders may prevent action if it hurts their interests, which further limits options for action. The one advantage of a reactive policy is that the greater temporal and public pressure may create also create greater incentive to act, whereas actively proactively allows for procrastination due to uncertainties about the future.

Emerging technologies create uncertainty not only because they themselves change, but because they change the environment in which they exist. New technologies can change the way people interact and go about their lives. They can change industry structures; they can change government policies and regulations. For example, the popularity of cell phones has fundamentally altered how many people both use and think of telephones. They are now mobile platforms not only for talking, but for emailing, texting, listening to music, and even watching videos or surfing the Internet. Many people have substituted their cell phones for traditional

[1] By its indirect role, I refer to primarily to the regulatory environment, but also to factors such as political stability, a level playing field, a framework of law, the banking sector, education, availability of funding for basic research, and incentives for investment. A direct role in technological innovation—a "push strategy"—would include actions such as legislation or regulation mandating the creation of new technologies or banning others.

landline telephones, which has decimated traditional telephony. Meanwhile, demand for bandwidth for cellular phones and other wireless devices has forced the government to rethink and retool its management of spectrum in order to accommodate new demand.

However, emerging technologies do not enter into static environments. The political, social and economic context they enter also changes independent of the technology, and these changes affect if and how the technologies become viable. Because this is a political science thesis, I choose to focus on how the role of government, and particularly on the regulatory environment. Most of the recent literature on the government and technology seems to focus on how government can either more successfully adopt and incorporate technology into performing daily tasks (computers at the IRS, e-government for greater openness), how governments can harness science and technology to better deal with scientific crises (mad cow disease), or how they can selectively promote key competitive technologies to boost economic growth.[2] The regulatory environment and how it affects emerging technologies seems to have fallen out of favor as a research topic.

The greater significance of this dissertation lies in understanding how government agencies' ability to anticipate emerging technologies and formulate appropriate policies affects the development of those technologies. That is, the regulatory environment matters. Government can foster technological innovation and competition by creating a friendly regulatory environment that is clear, stable, does not impose onerous or unnecessary regulatory burdens, and creates a level playing field. Alternatively, it can stifle innovation by doing the opposite.

The more interesting area, I believe, lies in the middle. Government can also shape emerging technologies—whether deliberately or not—by selectively imposing regulation on certain technologies or certain aspects of new technologies. The individuals and corporations that introduce new technologies, particularly corporations, are sensitive to regulatory environment. They may choose not to develop certain technologies, or leave out certain features, because they know that those are highly regulated, or because the competition has a too-cozy relationship with regulators, or more importantly, because they are afraid that the regulatory environment will change suddenly and unfavorably. This is where government foresight matters. Ideally,

---

[2] See, for example, OECD Staff, *Social Sciences and Innovation* (OECD, 2001), 108-114; J.V. Wood, "UK Foresight Programme—A Panel Chairman's View," http://www.nistep.go.jp/achiev/ftx/eng/mat077e/html/mat0774e.html (accessed January 6, 2008), and Vandana Chandra, *Technology, Adaptation, and Exports: How Some Countries Got It Right* (World Bank Publications, 2006).

government agencies would be able to foresee the direction of new technologies and proactively shape policies to promote their growth. Done reactively, it may be too late, because existing regulation may have already discouraged technologists from exploring certain areas. It may also have cut off options for the government, or allowed too much time for incumbent technologies to build an advantage.

In short, the ability of government agencies to anticipate new technologies and create an environment friendly toward their development is very important in maximizing the public good. Anticipation, or foresight, plays a critical role, because reactive policies can be too late and fail to lay the groundwork necessary for optimally fostering technological innovation. They may be time constrained, or otherwise not fully explore or allow for best options.

Theory

Literature

This dissertation speaks to a conventional wisdom on the ability of organizations, and particularly government, to exhibit foresight, rather than a specific body of literature. Put bluntly, there simply is not much literature on foresight in political science, and particularly not foresight with respect to technology. Despite the effort devoted to looking into the future and building strategy on a policy level within government agencies, and the volumes of five-year plans that populate the shelves of government agencies everywhere, mostly unread and ignored, the academic literature lags on the issue of foresight. The majority of the literature I reference is instead on organizational change and adaptation, since this literature is better developed. This literature applies particularly to the NSA case, due to the nature of the policy the Agency adopted and the long time period the case covers. To a lesser extent, due to some unexpected findings in the case on the FCC, it also speaks to the issue of regulatory inaction, which is an area of political science that also seems underexplored.

Foresight seems to have fallen out of favor as a research topic in political science over the past three decades, particularly with regards to technology. It is not entirely clear why this is true. Governments spend a lot of time and energy thinking about strategy and the future, yet very few agencies show any amount of foresight or even understanding of the role government plays in shaping emerging technologies. In terms of discussion of technology, most of the literature seems to take technology as exogenous, which by definition means that government response

must be reactive. Even much of the literature on technological innovation, while not taking technology as exogenous, does not look at foresight in the regulatory environment.

The conventional wisdom in political science, much of it derived from organizational and bureaucratic theory, says that organizations do not show foresight. Organizations resist change, and tend to do so only in response to crises and direct threats to their mission or autonomy. They do respond to change to changes in the external environment, including technology or economic changes, but slowly and reluctantly.[3] Much of this resistance to change is attributed to the routinization function of bureaucracies, which under static conditions are more effective by creating stability and reducing uncertainty in action. Foresight, on the other hand, requires proactive change – that is, changing in response to conditions which have not yet occurred – which clearly runs counter to a belief in organizational inertia.

Another explanation for the reluctance of government agencies to change that is often cited is regulatory capture. Much of the research on regulation in the middle of the 20th century looked to capture, where long interaction leads to regulatory agencies designing regulation to lock in benefits to a particular firm or industry, as an explanation for the problems of regulation. "If nearly a century of regulatory history tells us anything... it is that the rules-making agencies of government are almost invariably captured by the industries they are established to control."[4] Studies of the Federal Communications Commission, the Civil Aeronautics Board, and the Interstate Commerce Commission all seemed to confirm this belief. Economists who examined these agencies argued that regulation itself often inhibited technological innovation.[5] George Stigler offered what is now perhaps the best-known statement of capture, which argued that it was not something inherent in the commissions themselves that led to capture, but that capture was a reflection of prior political power, which created a regulatory mechanism (e.g., a

---

[3] James Q. Wilson, "The Politics of Regulation," in *The Politics of Regulation*, ed. James Q. Wilson, 357-394 (NY: Basic Books, 1980); James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989), 221; Aaron Wildavsky, *Speaking Truth to Power: The Art and Craft of Policy Analysis* (Boston: Little, Brown and Company, 1979), 217-218; Graham Allison, "Conceptual Models and the Cuban Missile Crisis," in *American Foreign Policy: Theoretical Essays,* ed. G. John Ikenberry, 413-458 (New York: Longman, 1999).

[4] Robert L. Heilbroner, et.al., *In the Name of Profit* (Garden City, NY: Doubleday, 1972), 239, cited in Thomas K. McCraw, "Regulation in America: A Review Article," *The Business History Review* 49 (Summer 1975): 164.

[5] All references drawn from review article by McCraw, "Regulation in America". On the FCC, Roger G. Noll, Merton J. Peck, and John J. McGowan, *Economic Aspects of Television Regulation* (Washington, D.C., 1973); Ronald H. Coase, "The Federal Communications Commission," *Journal of Law and Economics* II (October 1959): 1-40. On technological innovation, William M. Capron, ed., *Technological Change in Regulated Industries* (Washington, D.C., 1971).

commission, a quota system, or tariff schedule) to express itself.[6] James Q. Wilson argues that regulatory capture is a "simplistic" view of the politics of regulation, since agencies can be established with or without industry support. However, the agency regulatory climate created by the agency "acquires a life of its own." Even though some are hurt and other helped, the regulation creates stability and predictability, and therefore the industry as a whole comes to support the status quo because it reduces uncertainty.[7]

An interesting phenomenon that arises in FCC case study is their policy of forbearance, the deliberate delay of action, or deliberate inaction, for a stated purpose. This seems to be a rather underreported phenomenon in political science. There is an understandable tendency to select for cases where there is much activity, as it makes for easier proof of cause and effect. However, this creates a selection bias against cases where action is deliberately withheld. In the case of regulation, this may be a more interesting story – why forbear from exercising authority? For what purposes, and under what conditions might a federal (regulatory) agency choose to do so? To the extent that the political science literature covers regulatory inaction, the usual explanations centers on a lack of awareness of the issue, political stalemate, or bureaucratic inertia. That is, the inaction is not deliberate; it is not forbearance.

There are comparatively few explanations for deliberate inaction. As a general rule, the conventional wisdom in political science holds that regulatory agencies like to exercise their authority by regulating, and that expansion of bureaucratic turf is attractive if it can be done without threatening autonomy or the core mission of the agency.[8] One explanation for inaction that comes from conventional wisdom is 'duck and cover.' That is, faced with a controversial situation, an agency may choose to not make a decision rather than risk being blamed for making an unpopular or bad decision. The rationale is that it is easier to explain inaction than to face public scrutiny due to an unpopular and harmful action. I find this argument unconvincing, however, given the very public backlash that agencies have faced when they failed to act and disasters ensued. (Hurricane Katrina, intelligence failures)

---

[6] George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics and Management Science* II (Spring 1971): 3-21. Also Stigler, "The Process of Economic Regulation," *The Antitrust Bulletin* XVII (Spring 1972): 207-235.
[7] James Q. Wilson, "The Dead Hand of Regulation," *Public Interest* 25 (Fall 1971): 47.
[8] Wilson, *Bureaucracy.*

Another possible explanation for deliberate inaction is that incremental actions provoke less resistance. Rule-making may be unattractive to a regulatory agency that exists in a conflictual environment, whereas it is more effective and efficient in environments where the regulated parties largely agree with the purposes of the statutes. Under conditions of conflict, agencies may favor incremental action or even inaction, since a series of small changes is less likely to provoke resistance. A case-by-case approach allows for incremental development of policy, since each small decision does not establish as much policy and therefore draws less opposition.[9] That is, if the stakes are small, interests that stand to lose are less likely to be able to organize to resist the changes.[10] This explanation seems plausible for situation in which there are many several powerful and evenly matched stakeholders with opposing interests.

Another potential explanation for forbearance is Wilson's discussion of regulatory discretion. Wilson argues that power for bureaucracies comes in the form of regulatory discretion, which gives them leverage (a bargaining chip) against the regulated. As such, they will avoid developing general rules in order to preserve discretion, since codification limits discretion. Wilson also notes that agencies may also have several goals rather than just one, and may favor discretion in order to tip results toward one or another favored result in each case. That is, "the general desire to realize a particular state of affairs is more important to the agency than the desire simply to insure that the rules are followed."[11] Both of these conditions would lead to deliberate inaction.

Expectations and Findings

Although the conventional wisdom would expect neither the NSA nor the FCC to show any foresight with respect to the emerging technologies of mass market encryption and VoIP, it turns out that both agencies were able to exhibit foresight. The NSA and FCC both anticipated the changes that their respective technologies would bring, and both adopted flexible policies that allowed them to accommodate technological, political, and economic uncertainties. As for adaptation, the NSA showed considerable tactical flexibility in terms of methods used to achieve its goal of slowing down the deployment of mass market encryption. The FCC, on the other hand,

---

[9] William West, "The Politics of Administrative Rulemaking," *Public Administration Review* 42 (September-October 1982): 425.
[10] Mancur Olson, *The Logic of Collective Action* (Cambridge: Harvard University Press, 1965).
[11] Wilson, "Dead Hand," 51.

did not seem to need to show tactical adaptation due to the nature of its policy of forbearance. That is, the conventional tools of bureaucratic delay seemed largely sufficient to allow for inaction until outside pressures forced action. In broad terms, the FCC's inaction on VoIP even in the face of pressure from incumbent telecommunications providers contradicts the conventional view of the FCC as an agency captured by the telecom industry. It also contradicts the conventional wisdom on how agencies like to regulate their authority by exercising their regulatory powers. However, the actions of the FCC do seem to fit the smaller subset of literature on regulatory inaction for the purposes of preserving regulatory discretion.

Methodology, Selection of Cases

Two cases are examined in this dissertation. The current focus of this dissertation, namely the question of the conditions under which government organizations are able to show foresight with respect to emerging technologies, was not the original question for which the two cases were selected. This is why the cases are not entirely comparable. However, I believe that the cases are sufficiently similar to draw the limited inferences that I do. Moreover, each case spans a long enough time period and contains sufficient within-case variation due to multiple sub-cases to alleviate the problems associated with using only two cases.

The first case is a longitudinal study of U.S. cryptography policy from 1973 to 1999, focusing on the NSA. The quarter-century period covered allows for in-case comparison due to the two distinct periods of NSA strategy and external conditions that exist. The first period runs from 1973 to 1991, during which export controls on encryption arguably reduced the availability of strong encryption and had national security benefits. After 1991, with the release of a freeware strong encryption program called Pretty Good Privacy (PGP) over the Internet, the export controls did not really achieve the purpose of restricting access to strong encryption, since it was so easily downloaded over the Internet. I believe that the NSA's foresight and development of a strategy to manage the development of commercial encryption technologies begins at some point in the late 1970s to early 1980s, but its largest shifts in tactics began after 1991. Implicitly, the NSA case also covers the period before 1973 to establish a baseline of behavior and external environment, namely that the NSA held a virtual monopoly on cryptography and no export or outside development was allowed.

The second case is a study of the FCC's management of Voice over Internet Protocol (VoIP) from the early 1990s to present. Several areas of regulation that potentially apply to VoIP are examined: disability access, 911/ Enhanced 911, intercarrier compensation, universal service, and the Communications Assistance for Law Enforcement Act (CALEA). These five sub-cases allow for examination of variation in VoIP policy as well, since some of these issues remain unresolved, others are partially resolved, and others largely settled. VoIP is an ongoing case, but I have attempted to keep up with the changes in FCC regulation so they are as up-to-date as possible.

I originally selected the cases intending to investigate how the timing of government regulation in the development process of emerging technologies affects the decision-making of technical designers, the final form of the technology, and if and how it is adopted commercially. Previous research into export controls on cryptography had led me to conclude that the NSA's early and active intervention had reduced the quality of encryption built into mass-market software, and had probably also delayed its production and adoption by several years. The intent was to examine how inventors and corporations evaluated and incorporated technical, political and economic uncertainty into their designs. However, I soon discovered that I lacked both the technical capacity to play the technological what-if game and the access to decision-makers to be able to pursue that line of inquiry competently.

In looking into the FCC's lack of regulation of VoIP—the FCC had not yet begun to regulate VoIP when I began my research four years ago—I sought to use VoIP as an example of how a technology develops when government regulation comes only late in the development process. I had assumed that the FCC had not gotten around to regulating VoIP. Instead, I discovered that the Commission was quite aware of the technology and had long ago very deliberately decided to hold off on imposing regulations. This seemed curious, especially given the conventional wisdom in political science that regulatory agencies like to regulate.

My discovery of the FCC's policy of forbearance, formed relatively early in the development cycle of VoIP, echoed my surprise in finding the 'slowing down encryption' strategy adopted quite early on by the NSA. The realization that the NSA's seemingly ham-handed actions with respect to trying to suppress commercial cryptography were actually the outer face of a far subtler and more nuanced strategy to preserve and extend its existing technological advantages while building up its own capabilities had been one of the most

fascinating aspects of the research for my master's thesis. Now I had found something similar, although not entirely comparable, in an agency with a very different function. This is how the focus of the dissertation came to be on the question of government regulatory foresight.

Sources are a combination of primary and secondary source documents. Both cases rely heavily upon government documents. In the NSA case, secondary sources dominate, given the difficulty of accessing information on the Agency. It is supplemented with Congressional testimony and proposed laws and bills to the extent possible. The FCC case is largely built upon FCC records and documents, particularly the records of Notices of Proposed Rulemaking (NPRM), the comments on those NPRMs, Orders and Memoranda, and the statements of the various Commissioners.

Summary of Findings

Both the NSA and FCC showed foresight in their management of their respective technologies of commercial encryption and VoIP. Both agencies looked forward and anticipated the direction that each technology would take in its development and formulated flexible policies that would allow them to best manage the technologies to achieve their goals. I identify three characteristics of each organization that allowed them to competently anticipate and prepare for the technologies. First, the importance of technology in both agencies' missions gave them an incentive to 'stay ahead of the curve' with respect to technologies. Second, both had a lot of experience managing technologies and dealing with technological change and uncertainty, so both understood the need for flexible policies. Lastly, both agencies were expert in their technologies and recognized the limits of their knowledge, so they did not try to overreach in what they tried to achieve. The chief differences in the two agencies' approaches seemed to stem from differences in their missions and in their level or type of technical expertise.

For the NSA, recognizing that the beginnings of commercial encryption meant that its old strategy of maintaining a functional monopoly on cryptography would no longer work required some foresight. The NSA seems to have realized fairly early, perhaps at some point in the early 1980s, that maintaining strict control over encryption technologies through a combination of export controls, secrecy orders, and other mechanisms would be impossible. Instead, it seems to have shifted to a strategy of trying to slow the spread of mass market encryption, the widespread

adoption of which would complicate their work by increasing the amount of encrypted traffic, and building up and solidifying the NSA's existing technical advantage.

Since its founding, the NSA was the undisputed leader in encryption technology in the U.S., which meant that much of the ground covered by commercial encryption beginning in the 1970s was likely familiar territory. More importantly, as an agency whose ability to execute its duties depended upon being at the forefront of technology, the NSA had experience dealing with new technologies. It knew that it would not be able to predict the exact form or timing of commercial encryption, nor how the industry would look, but it could manage and shape it. The NSA leveraged its experience and its technical expertise to formulate a new strategy to best protect its interests while allowing for the flexibility that dealing with the uncertainties commercial encryption would bring. Doing so required not only a willingness to look forward and act upon those findings, which conventional wisdom says is unusual for organizations, but also a willingness to move away from historical behaviors and tactics. The NSA began a reluctant shift away from complete secrecy to a degree of engagement with the academic community and the public in order to execute this new strategy. It also recruited bureaucratic allies such as law enforcement, which it had never done before, or at least not publicly.[12] Bringing law enforcement on board allowed them to reframe their argument in terms of fighting crime rather than just as preserving national security, an acknowledgement of the changing political climate after the end of the Cold War. The NSA also showed some adaptation in its willingness to submit proposals for federal standards such as the Digital Signature Standard, although its record on this point is mixed.

The FCC also showed foresight in its approach to regulating VoIP. Like the NSA, the Commission showed an unexpected willingness to not only look forward but to act—or rather, to deliberately *not* act—on the results of that projection. The FCC relied upon its experience with other emerging communication technologies, which had taught it to recognize both the uncertainties that emerging technologies create and the dangers of regulating too early. Instead, the FCC adopted a policy of forbearance, holding off from imposing legacy regulations on VoIP in order to allow the technological, economic, and other uncertainties to resolve themselves as

[12] Presumably, the NSA always had friends within the defense establishment, but given the secrecy that surrounds much of the NSA's activities during, it is hard to tell to what extent they were influential in advocating favored policies. Certainly I could not find evidence of anything similar to the very public lead that the FBI took in advocating Digital Telephony and the Clipper Chip in the history of the NSA or its presumptive agency/ organizational allies.

VoIP matured. The added impetus of its mandate to promote competition by fostering innovation probably reinforced this cautious approach. The FCC recognized that the potential for the "dead hand of regulation": that is, it is easier to regulate at a later date than to undo regulation. It also recognized that preserving some degree of regulatory flexibility would enable it to regulate more effectively in the future.

Adopting a policy of forbearance seems not to have been as antithetical to organizational culture as moving away from secrecy was for the NSA. However, it did require a regulatory agency to very deliberately *not regulate,* which runs counter to the conventional wisdom that regulatory bodies regulate because that is what they do. The NSA and FCC both used traditional tools of bureaucracies, particularly that of asserting bureaucratic turf, to further their own policies. However, while the NSA did so in order to impose regulation and micromanage, the FCC did so in order to *prevent* regulation, instead fencing off VoIP to protect it from state regulators. The FCC eventually began regulating certain types of VoIP in 2003. There are two possible explanations, which both seem to be at least partially true: first, that the technology had matured and stabilized enough to begin regulating without fear of stifling innovation; and second, because of external political pressure, particularly from law enforcement on CALEA.

The differences in their approaches to technology management seem to stem largely from the different roles each agency played as well as their own confidence in their knowledge of the technology. The NSA took a hands-on approach to managing commercial encryption, arguably micromanaging some aspects of the technology through the standards review and export controls processes, whereas the FCC chose a hand-off policy and instead encouraged inventors to innovate. The NSA probably perceived itself as facing less technological uncertainty than did the FCC due to a combination of technological superiority vis-à-vis commercial cryptography and the lead time in previewing new cryptographic developments that the export control review process granted the NSA. The NSA also had an obvious interest in suppressing the technology, since widespread use of encryption exponentially complicated its ability to fulfill its mission, which the FCC lacked as an ostensibly neutral regulatory agency. The greater technological uncertainty, coupled with the more difficult task of promoting rather than discouraging technological innovation, may well account for the FCC's more cautious policy of forbearance.

Roadmap

This dissertation contains five chapters. This first chapter introduces the question and theory. The second is a narrative of the history of the National Security Agency's management of commercial encryption technology. The third chapter looks at the Federal Communications Commission's management of Voice over Internet Protocol. The fourth chapter analyzes the similarities and differences between the cases. The final chapter concludes the dissertation, identifies policy implications, and proposes areas where more research is required.

This page deliberately left blank.

Chapter 2
Cryptography and the National Security Agency[13]

Introduction

This chapter examines how the NSA managed encryption technologies during the period from the 1970s through 1999.[14] Contrary to conventional wisdom, the NSA did not sit back and merely react to the emergence of mass market commercial encryption, which threatened its ability to easily monitor communications. Rather, the NSA proactively leveraged its superior technical understanding to formulate a surprisingly subtle strategy to preserve its ability to successfully monitor communications and manage the uncertainties that mass market encryption presented. The strategy the NSA ultimately adopted was to slow down and limit the widespread adoption of encryption software as much as possible—not, as it appeared, to prevent it altogether. A secondary strategy was to weaken the encryption software that did make it to market. These strategies served two purposes: first, it would reduce the quantity and strength of encrypted communications, which would make monitoring and decrypting communications easier; and second, it would buy the NSA time to increase and solidify its existing technical advantages.

Much of the territory academic and commercial cryptography covered during this period was likely ground the NSA had already explored within its own walls. In other words, the NSA probably worried less about a direct threat to its cryptanalysis abilities than the compounded inconvenience of millions of users automatically encrypting their communications with built-in strong encryption software. Thus, despite this story taking place during a period of immense technological innovation, with the development of personal computing, the Internet, and even major breakthroughs in cryptographic research such as the discovery of public key cryptography, the real issue was not one of managing technological uncertainty. Rather, the significant uncertainties lay in the economic, social, and especially political realm.

The NSA adapted its tactics quite adeptly to the new environment. The end of the Cold War shifted the political environment in which the NSA operated. It reduced the perceived external security threat and thereby shifted the balance of national values away from national security and toward other interests such as economic growth. The growth of the newly powerful

---

[13] The bulk of the content of this chapter is drawn directly or indirectly from my master's thesis. Shirley K. Hung, "U.S. Export Controls on Encryption Technology," (Master's thesis, Massachusetts Institute of Technology, 2004).

[14] By encryption technologies I refer to non-military encryption technologies, specifically those in the public sector such as the federal encryption standard(s) and commercial, usually mass-market, encryption technologies. Obviously the NSA's duties and expertise extend far beyond this limited realm.

computer software industry, e-commerce, and even computing-focused civil liberties groups further complicated the NSA's management of cryptography. However, the NSA did not allow these new challenges to deter it from preserving its organizational interests. It shifted away from its older, somewhat ham-handed tactics of restricting cryptography, which had included everything from secrecy orders, bureaucratic turf battles with other government agencies, regulatory capture of Congressional committees, micromanaging of encryption standards, and of course the export control review process. Instead, it adopted a much subtler tactic. In the 1990's the NSA began recruiting organizational allies in law enforcement, especially the Federal Bureau of Investigation (FBI). This allowed the issue of restricting commercial encryption and maintaining access to communications to be reframed as the more politically palatable and significant issue of fighting crime and preserving domestic security, rather than as a Cold War-era national security issue. Meanwhile, it allowed the NSA to get out of the political limelight and focus its attention on its area of expertise: building up its technological advantage.

Summary of Events

The most striking part of the story of encryption regulation is the NSA's unspoken strategy of delaying and limiting the widespread use of commercial encryption in order to make monitoring communications easier. The second interesting feature is the tactical adaptability the NSA exhibited in executing this strategy. The sheer variety of mechanisms the NSA employed to keep both information about encryption and actual encryption technologies from becoming widespread is actually rather impressive. More so, however, is that the NSA was able and willing to recognize a need for a change in objectives and make the tactical changes necessary to achieve them. This required a degree of foresight and flexibility that does not fit in with the conventional wisdom about organizations.

From its creation in 1952, the NSA had a virtual monopoly on serious cryptographic knowledge, and it worked very hard to maintain that control. It operated in secrecy, with national security through signals intelligence as its raison d'être. For the first two decades of its existence, it succeeded, with two notable exceptions. The first was the very public defection of two NSA cryptologists to the Soviet Union in 1960. The other was the publication of *The Codebreakers,* a book on the history and techniques of cryptography that included the first public account of the NSA's capabilities.

The NSA's virtual monopoly on cryptography began to break down in the early 1970s. The merging of computers and communications created a demand for encryption in highly specialized civilian sectors such as the financial services industry. The government, too, recognized the need for an encryption standard, which led to the National Bureau of Standards (NBS) publishing a solicitation in the *Federal Register*. Although the NSA did not submit a proposal, it became intimately involved in the design and development process for the IBM product that eventually became the Digital Encryption Standard (DES). By some accounts, the NSA forced changes, including shortening the length of the encryption key, that weakened the standard.

Meanwhile, independent cryptographers discovered the principle of public key cryptography. This enabled individuals who had never met to communicate securely, thereby solving the historical problem of key distribution and made effective encryption much easier to use. The discovery of the principle of public key also led to the development of one of the most popular encryption algorithms in use today, the RSA algorithm.

The breakdown of the NSA monopoly over cryptography drove it to try to re-secure its control, with limited success. The NSA engaged in a protracted turf battle with the National Science Foundation (NSF) over the exclusive right to fund and thereby control cryptographic research during the latter half of the 1970s. The NSA also attempted to impose secrecy orders on various inventions or prevent publication of papers related to cryptography, only to be forced to back down due to negative publicity. Even its historically good relationship with Congress, one which might arguably be characterized as Stiglerian capture of intelligence oversight committees, began to break down. In a disturbing parallel to today's headlines, Congress began investigating instances of warrantless surveillance of US citizens by the NSA.

The NSA's attempts to reassert control over cryptography continued in the 1980s with mixed success. In 1982, the NSA engineered a Presidential Directive under Reagan that granted authority over all US information systems to the NSA. However, the Directive was withdrawn after Congress opened hearings into the matter, viewing the Directive as an encroachment on Congressional authority. A few years later, when the Democratic Congress granted jurisdiction over civilian cryptography to the National Institute of Standards and Technology (NIST) in the Computer Security Act of 1987, the NSA performed a bureaucratic end-run by signing a memorandum of understanding with NIST that created a NIST/NSA technical working group for

civilian cryptography—thereby circumventing Congressional intent to grant sole jurisdiction to NIST. Meanwhile, an attempt to replace DES with a new standard failed due to lack of cooperation from the banking industry. However, the NSA succeeded in having its Digital Signature Standard adopted as a federal standard.

On the commercial front, the 1980s marked the first time a mass market software program, Lotus Notes, included built-in encryption. The NSA succeeded in using the export control review process to force Lotus to use weaker encryption algorithms and shorter keys and delay shipment of the product by several years. However, Lotus Notes was a harbinger of the world to come: easy, ready access to encryption for the average user.

The 1990s brought a new series of challenges for the NSA. Technologically, the growth of the Internet and its potential as a distribution channel for encryption software clearly posed the biggest threat to the NSA's ability to limit the use of encryption. The release of the free software program PGP (Pretty Good Privacy) on the Internet largely eliminated significant barriers, whether financial or technical, to access to strong encryption. The popularity of personal computers ate into the near-monopoly on computing power the NSA had held for decades. Economically, the growth in e-commerce increased demand for encryption to secure financial transactions, which would clearly create additional work for the NSA. The growth of the computer hardware and software industries, too, created new actors with interests diametrically opposed to those of the NSA. The computer industry learned that its money could buy influence and a voice in Congress that could chip away at the cozy relationship the NSA had once enjoyed with select committees. Socially, computer-savvy civil libertarians began agitating for a loosening of restrictions on cryptography. Underlying all of these changes was the end of the Cold War, which reduced the perceived national security threat and undercut the urgency of the national security argument for restrictions on strong encryption. (See Figure 2.1 for a Summary of Changes in External Environment for Encryption.)

		Time Period		
	Characteristic	**Pre-1973**	**1973-mid 1980s**	**Mid 1980s-1999**
Technology	Monopoly on cryptography	Yes	Limited	No
	PC revolution	No	Yes	Yes
	Internet	No	No	Yes
Economics	Commercial encryption	Limited institutional users	Lotus Notes; Limited other programs	Widely available over Internet, built into software
	Software Industry/ Lobby	No	Beginning	Yes
Social	Digital Civil Liberties movement	No	No	Cypherpunks, EFF, CDT, etc.
Judicial	Judicial Involvement	No	DOJ: ITAR unconstitutional-opinion not circulated	*Bernstein v. US; Junger v. Daly; Karn v. US*
Political	International	CoCom	CoCom	CoCom; Wassenaar
	Congressional interest	Intel committees only	Intel committees only	Various proposals to liberalize export control regime, etc.

Figure 2.1. Characteristics of External Environment for Encryption by Time Period

To its credit, the NSA recognized that the change in external conditions warranted a change in tactics. To this end, the NSA expanded its repertoire of tactics to include a variety of political means as well as technological solutions. In line with its status as the nation's premier cryptographic agency, the NSA proposed a new solution: the Clipper Chip. It would use all the technical expertise of the NSA to produce a strong encryption algorithm for widespread use, with one hitch: it would contain a 'backdoor' for law enforcement. The 'backdoor' would provide a technological means for law enforcement, provided they had appropriate warrants and authorization, to decrypt communications encrypted with the Clipper Chip.

To push this new agenda, the NSA recruited allies such as the FBI, which brought a more politically palatable law enforcement angle to the debate. (Although still strong, the national

security argument was difficult to sell domestically, given that most users of the Clipper Chip would be U.S. citizens. In addition, the end of the Cold War and consequent reduction in perceived external threats made national security arguments seem less urgent.) At the urging of the NSA, the FBI then introduced initiatives of its own, including a wiretapping bill called the Digital Telephony proposal that eventually became the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA features prominently in both this and the next chapter.

The NSA moved beyond its traditional political allies in the intelligence committees in Congress to lobby the incoming President Clinton and the technophile Vice President Gore to support the Clipper Chip. The agency even went so far as to break out of its traditional shell of secrecy to engage with the civilian cryptographic community, openly attending cryptography and mathematics conferences rather than trying to shut them down.[15]

Although the Clipper Chip initiative was ultimately unsuccessful, and export controls on encryption were loosened considerably in 1999, the efforts were arguably quite effective in terms of delaying development and deployment of other forms of cryptography. It is impossible to quantify how many years' delay resulted, or how much more encryption and of what strength or quality would otherwise be used today. However, the fact that the NSA bought itself time by throwing what seemed like the kitchen sink at commercial cryptography is undeniable. This would not have been possible without the existence of and willingness of key members of the Agency to formulate and pursue a rather sophisticated and unspoken long-term strategy for managing mass market encryption. While to the casual observer it may have seemed that the NSA sought to eliminate strong commercial encryption altogether, the agency most likely never expected such a strategy to work. Instead, it used a variety of tactics as stalling devices, never expecting for them to actually succeed, to buy itself time to increase and solidify its existing technological advantages.[16] These tactics were also directed at making commercial encryption

---

[15] Although one could argue that attending the conferences was simply another way to gather more information and possibly recruit cryptographers.

[16] That said, had any of the various tactics employed actually succeeded, I doubt anyone at the NSA would have complained. This is particularly true of the ultimate failure of the Clipper Chip. It is uncertain whether the NSA actually expected the Clipper Chip to go into widespread use, although its political partners, the FBI, DOJ, etc, clearly very much hoped and perhaps even expected that the Clipper Chip would become standard. Based on past evidence, and on events currently emerging, it seems that the NSA, unlike the other agencies, always had a trick up its sleeve: after all, alone among the agencies involved, it had the raw computing power and technical expertise to break sophisticated codes even without the shortcut of the Clipper Chip's backdoor. See Bruce Schneier, "Did NSA put a Secret Backdoor in New Encryption Standard?" *Wired*, November 2007,

weaker, more difficult to use, and less widely available, with the objective of reducing the number of users.

Each stage of the development of 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 and preserve its own dominance in the field. It is not clear at what point the NSA adopted the strategy of simply slowing the use of encryption rather than actively preventing it. However, by the mid-1980s and certainly by the early 1990s, its actions suggested a shift toward constraint rather than containment of encryption. This most likely stemmed from the recognition that containment would be impossible given the way encryption and supporting technologies (PCs, the Internet) were evolving. It was also during the 1990s that the agency began to adapt to a new political environment, moving away from a long-established tradition of avoiding publicity in order to better argue its case for continued restrictions on encryption. (See Figure 2.2 for a table of NSA Actions)

---

http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115 (accessed November 17, 2007). The article questions whether the NSA inserted a 'backdoor' into the latest federal standard through the random number generator (RNG).

	Time Period		
Characteristic	**Pre-1973**	**1973-mid 1980s**	**Mid 1980s-1999**
Standards setting process	No	DES	CCEP; DSS; Clipper Chip– submit proposals
Export control review process	Yes	Yes	Yes
Secrecy orders, classification	Codebreakers	Meyer letter; Davida and Nicoli patents	Merkle paper; textbooks
Bureaucratic turf battle	N/A	NSF, NIST, Poindexter Directive	NIST
Recruit bureaucratic allies	No	No	FBI/ DOJ; DEA
Approach incoming administration	?	?	Yes
Public debate/ engagement	No	Beginning	Yes

Figure 2.2. Summary of NSA Actions by Time Period

Roadmap of Chapter

The rest of this chapter is a narrative of the NSA's approach to cryptography outside its walls gradually shifted from a strategy of suppression to management during the period from the 1970s to 1999. In particular, I discuss how the NSA pursued two objectives with respect to commercial cryptography: first, to slow down mass market adoption of encryption, and second, to control and weaken the encryption that was produced. This two-prong strategy would minimize the impact that commercial cryptography had upon the NSA's ability to monitor communications as well as buy it time to build up its technological capabilities.

This second half of the chapter discusses the NSA's tactical adaptations, and how it broke away from long-held traditions of silence and secrecy. During this period the NSA found political allies and proposed technical solutions in order to continue pursuing its ultimate strategy of slowing down and controlling civilian cryptography. This shift away from established practice suggests that under certain conditions, organizations are able to adapt, and even be proactive, in responding to emerging technologies.

The first section explains the origins of the NSA and its organizational culture. The second section discusses technical developments including the Digital Encryption Standard and public key cryptography. The third section discusses the early history of the NSA's interactions with Congress, other government agencies such as the National Science Foundation (NSF), and the public. The fourth section very briefly discusses the introduction of the first popular mass market computer software that included built-in encryption, Lotus Notes. The fifth section returns to the NSA's attempts to influence government policy during the final years of the Cold War, when the NSA had already begun its strategic shift from an attempt to suppress mass market cryptography to simply attempting to slow its development.

The sixth section discusses the political, technological, and social changes in external environment due to the end of the Cold War, the development of free encryption software distributed over the Internet, and the rise of the digital civil libertarian movement. The seventh section discusses the new Clinton administration's attempts to formulate a national encryption policy and the NSA's attempts to influence that policy. The eighth section covers the technological-social developments of the period, during which the newly created digital civil liberties groups conducted a series of highly publicized 'hacks' of various encryption algorithms both for entertainment and to prove the political point that export controls were being put on rather weak cryptography. The ninth section discusses the Clinton administration's attempts to gain international cooperation in imposing export controls on encryption software through the Wassenaar Arrangement. The tenth and final section concludes the chapter with an examination of the beginning of liberalization of encryption policy, primarily through the involvement of Congress.

Section 1. National Security Agency History

Formation of Organizational Culture

The conditions under which the NSA was created, combined with the importance of its mission, led to the development of a mentality in which national security, secrecy, and maintaining a technological edge and control over cryptography were one and the same. The NSA emerged out of a series of wartime agencies. In both World War II and the Korean War, intelligence failures had led to disasters. The NSA's establishment right at the start of the Cold

War reinforced its wartime mentality and its belief in the importance of its mission in a time of external security threats. However, as external political conditions began to shift toward détente and eventually the end of the Cold War, and the NSA's control over cryptography began breaking down in the 1970s, it was able to move away from its emphasis on maintaining a monopoly on cryptography. Rather, it showed some sensitivity to the unavoidable existence of cryptography in the commercial sector and changed its ultimate goal and tactics toward simply reducing and slowing the use of encryption instead of eliminating it altogether.

The NSA owes its existence to a series of intelligence failures during World War II and the Korean War. During World War II, Army intelligence agencies had intercepted information about the Pearl Harbor attack almost eight hours prior to the attack. Due to a lack of coordination between the armed services' respective intelligence agencies, however, warnings of the impending attack did not arrive at Pearl Harbor Navy headquarters until six and a half hours after the attack. Congressional investigations into the debacle and the pressures of coordinating burgeoning wartime 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 (COMINT) functions and responsibility for coordination of the various COMINT agencies, and added State Department cryptosystems to its list of responsibilities.[17] However, 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. Even though the interagency oversight committee ranked Korea the fifth most volatile area of the world, the notice to target Korea for intelligence did not reach AFSA due to bureaucratic miscommunication. Furthermore, the agency was not set up to handle Korean traffic once the invasion occurred.[18] Consequently, 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

[17] Individual agencies retained tactical communications intelligence responsibilities, which are best done near the point of combat, and low-echelon communications security.
[18] James Bamford, *Puzzle Palace* (Boston: Houghton-Mifflin, 1989), 49-50.

almost in their entirety in a Presidential directive in November 1952 that created the NSA to replace AFSA.

The NSA's origins 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 into its formative years in the Cold War. The immediate transition from WWII into the Cold War reinforced the mentality, because the lack of communication between the U.S. and Soviet Union meant that one of the only ways to gather information about the other was through monitoring of signals intelligence. It 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."[19] 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."[20]

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

[19] David Kahn, *The Codebreakers* (New York: MacMillan, 1967), 690.
[20] Bamford, *Puzzle Palace*, 43.

served to validate its 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]"[21] What this meant was that unlike every other individual and agency in the U.S., laws governing the gathering of intelligence 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 a 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."[22] 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." [23] 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.[24]

Nor did the traditional government check on agencies, the budget process, exist. For the first twenty-five years of its existence, the NSA dominated the intelligence budget, but without

---

[21] Department of Justice, "Prosecutive Summary," March 4, 1977, p. 12, quoted in Bamford, *Puzzle Palace*, 46.
[22] Bamford, *Puzzle Palace*, 4.
[23] *Ibid.* 4.
[24] *Ibid.* 46.

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 oversight. Estimates of the NSA's portion of the intelligence budget ranged from 85-90%.[25] 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).[26] 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.[27]

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 cryptographic 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.[28] If anything, it had

---

[25] 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 sess., 333-334; Lee Lescaze, "Pentagon vs. CIA: Control of Intelligence Community Sparks Major Institutional Battle," *Washington Post,* June 10, 1977, A1, cited in Bamford, *Puzzle Palace,* 2..

[26] Although cryptography is only a part of cryptology, I use the terms interchangeably. Technically, cryptology is the general term that encompasses both cryptography, the writing of codes, and cryptanalysis, the breaking of codes. 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, Britain's first official cipher bureau.

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

[28] 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,* 204, cited in Kahn, *Codebreakers*, 675.

embedded the importance of secrecy so deep into the organizational ethos that secrecy became almost an end unto itself.

One way to search for organizational culture, writes Edgar Schein, is through analysis of the process and content of socialization of new members.[29] By this standard, secrecy 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 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.'" [30] 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."[31]

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.[32] 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 national 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.[33] Although Petersen was given a seven year sentence

---

[29] Edgar Schein, "Coming to a New Awareness of Organizational Culture," *Sloan Management Review* 25 (Winter 1984): 3-16.

[30] Kahn, *Codebreakers*, 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 apparently replied, with total seriousness, "I cannot confirm or deny that we have computers at NSA."

[31] Steven Levy, *Crypto* (New York: Viking, 2001), 14.

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

[33] 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

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 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."[34] 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.[35] 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. Before these security breaches, secrecy had been a problem-solving behavior and therefore more easily adaptable; afterward, it became a top priority not only for practical purposes but for anxiety avoidance as well. 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

---

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, 1.

[34] Kahn, *Codebreakers*, 692.

[35] *Ibid*, 695.

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.[36] 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 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."[37] 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 tried very hard to prevent. The book contained the first public account of the extent of the NSA's capabilities, 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

[36] *Ibid*,, cited in Levy, *Crypto* 15.
[37] Levy, *Crypto*, 15.

had ever been compiled without an EYES-ONLY stamp on each page."[38] 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."[39] 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."[40] 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.

The Importance of Signals Intelligence and How It Works

The NSA's belief in the importance of its own mission, both in having secure ciphers and also in being able to read the communications of others, was not wholly a product of organizational hubris. The United States relies more upon signals intelligence (SIGINT) than any other type of intelligence.[41] As former Senate Intelligence Committee member Walter Mondale once stated, the NSA is "possibly the most single important source of intelligence for this nation."[42] 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

---

[38] Levy, *Crypto*, 23.
[39] Bamford, *Puzzle Palace*, 168. In the early 1980s, the NSA would try to suppress the publication of Bamford's *The Puzzle Palace* as well. See Whitfield Diffie and David Landau, *Privacy on the Line* (Cambridge, MA: MIT Press, 1998), 231.
[40] Levy, *Crypto*, 23.
[41] 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).
[42] U.S. Senate, 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., 35., cited in James Bamford, *Puzzle Palace*, 4.

has increased dramatically.[43] 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.[44] 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."[45]

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 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,

---

[43] 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), 143-190, see especially 186-188, and Robert Churchhouse, *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet* (Cambridge: Cambridge University Press, 2002). I have seen ULTRA erroneously referred to as MAGIC by some authors. MAGIC is the code name assigned to Purple-machine encoded from Japan, while ULTRA was limited to the European theatre.

[44] U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Foreign and Military Intelligence,* 333-334; Lee Lescaze, "Pentagon vs. CIA," cited in Bamford, *Puzzle Palace,* 2.

[45] National Security Agency, "Mission statement," http://www.nsa.gov/sigint/index.cfm (accessed January 21, 2008).

and other enemies of the U.S. would threaten American national security because it would reduce the speed, quality and quantity of SIGINT.

Section 2. Technical Developments

DES (Digital Encryption Standard)

One of the first signs that the cryptography would not stay behind the Triple Fence came in the form of a largely ignored solicitation for a standard cryptographic algorithm in the May 1973 *Federal Register.* The National Bureau of Standards (NBS) had submitted the solicitation in anticipation of the Privacy Act of 1974 and other federal laws, which in light of increasing use of computers, implied that approved cryptography must be available to government users other than NSA's traditional national security clients.[46] The solicitation 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 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.[47] During this period, the NSA still had a virtual monopoly and clear superiority in cryptography, and it believed the way to maintain it was to simply refuse to participate in efforts outside its walls. The NSA would come to regret this decision, however, when it decided that the NSA-modified IBM submission that became DES was too strong, and worse, too popular. Thirteen years later, the NSA would try to leverage its technical expertise and political connection to replace DES with a more NSA-friendly standard, to no avail.

The algorithm that became the federal Digital Encryption Standard (DES), and by extension the *de facto* standard for private industry and individuals, began life as the Lucifer cipher in one of IBM's research labs.[48] The Lucifer cipher and its product version were

---

[46] Diffie and Landau, *Privacy,* 59 and footnotes. Notably, the law made no mention of individual or private users, only of government users.

[47] Diffie Landau, *Privacy,* 59.

[48] 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".

originally designed for Lloyds Bank in London to secure their automated teller machines (ATMs) against telephone fraud.[49] 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.[50] 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-engineer the plaintext. [51] 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 cryptography, the key would provide all of the secrecy and security.[52]

Development of the DES system (officially called DSD-1 by IBM, but informally referred to still as Lucifer) continued for several years after IBM's initial submission. It

---

[49] 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!"

[50] 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.

[51] 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* 228 (May 1973): 15-23.

[52] 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.

strengthened Lucifer to eight substitution boxes and 16 rounds of transformations (permutation, blocking, expansion, bonding, and substitution with a digital key, repeated 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.[53]

Knowing this, the NSA used its reputation for technical superiority to influence the development of DES and keep it manageable. In early 1974, the NSA contacted IBM to propose a quid pro quo re Lucifer. The 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. (Shipments of physical items are easier to control. The leaking of the DES algorithm, as with the difficulty of controlling the spread of cryptographic code over the Internet two decades later, played a major role in forcing liberalization of the export control regime. It may also be what prompted the NSA to modify its goal to slowing rather than outright controlling the dissemination of cryptographic knowledge.) The NSA also informed IBM that it would restrict shipment of the chips to certain countries altogether, and that the chips could be exported only to approved countries, and only with a license, obtainable with a signed document from the customer promising not to re-export or re-sell the product.[54] 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 these export controls and restrictions, the NSA adhered to its established routine of favoring secrecy: it prompted the government to issue a secrecy order on Horst Feistel's Lucifer patent, making it a federal crime to publish on or publicly discuss Lucifer without written permission from the Commissioner of Patents.[55]

The origins of the NSA's strategy of weakening rather than eliminating encryption outside its walls may date back to this period. During the process of putting Lucifer onto a chip, the original 128-bit key size was cut down to 56 bits, weakening the encryption. There continues

---

[53] Levy, *Crypto*, 48.

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

[55] 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.

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."[56] 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.[57] 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.[58] 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 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

---

[56] Whitfield Diffie, "Preliminary Remarks on the National Bureau of Standards Proposed Standard Encryption Algorithm for Computer Data Protection," May 1975, quoted in Levy, *Crypto*, 38.
[57] Levy, *Crypto,* 37-65.
[58] *Ibid.* 58-60.

had more and more powerful computers than anyone in the world.[59] 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 as 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.[60] 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 seems to have been a result 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.[61] 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, an

[59] *Ibid.* 63.

[60] 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 Wildavsky, *Speaking Truth to Power*, 215.

[61] Much like the uproar over NSA wiretapping during 2006-7, in 1975, Senate Intelligence Committee hearings revealed an NSA effort to monitor domestic communications named "Project Shamrock", for which the agency was roundly criticized.

encrypted message could be re-encrypted ad infinitum. The Triple DES variant that emerged a few years later required breaking *three* keys rather than one to decrypt.

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.[62] 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 then programs 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 are then be read and analyzed. Thus gathering and analyzing SIGINT requires that all communications be readable. With the use of strong encryption, this is 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 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 it was around this period that the NSA 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 rendered them functionally the same as plaintext). 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

[62] See Kahn, *Codebreakers*, 672-736.

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.[63]

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."[64]

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, a cryptographic conference, "It's not that we haven't seen this territory before, but you are covering it very quickly."[65]

Understanding the likely development trajectory of cryptographic knowledge and technology outside of the NSA, an understanding possible because of the agency's dedication and superior technical capabilities, allowed it to formulate a strategy to cope with the inevitable spread of encryption in the 'outside' world. The agency probably realized what was coming long

---

[63] Diffie and Landau, *Privacy*, 105-6.
[64] Levy, *Crypto,* 156.
[65] Diffie and Landau, *Privacy*, 239.

before anyone outside of its walls did, and this early recognition – and the willingness of its leadership to act upon it to protect the organization's interests – shows remarkable foresight that contrasts with the stereotype of the purely reactive, unchanging organization.

Public Key and RSA

The following section discusses the details of the development of public key cryptography and one of the best-known encryption algorithms in use today, the RSA algorithm. The discovery of the principles behind public key cryptography was important because it made it possible for people who had never met to exchange secure communications, thereby eliminating a security and logistical roadblock to widespread use of cryptography. Before the principle of public key cryptography was discovered, cryptography had only used symmetrical keys. Symmetrical keys required the sender and receiver to each have a copy of the key in order to encrypt and decrypt a message. This in turn required a secure key distribution system: either the sender and receiver had to meet, or some other way of getting the same key into the sender and receiver's hands had to exist. The key distribution was the weakest link in the chain, the obvious target for anyone seeking to break into secure communications. Public key cryptography eliminated this weak link, thereby revolutionizing cryptography.

The RSA algorithm is one of the best-known implementations of public key cryptography. It is important because it was the first algorithm that could both sign (to verify identity) as well as encrypt (to verify content) communications. The inventors, three professors at the Massachusetts Institute of Technology (MIT), realized that they could fulfill the mathematical requirements of public key cryptography by relying on the difficulty of factoring large numbers into their component primes, a problem that has plagued mathematicians for millennia. Today the RSA algorithm is widely used in electronic commerce, particularly for securing the credit card numbers of online shoppers.

The reader less technically inclined can skip the rest of this section.

Soon after the adoption of DES as the federal standard, two independent cryptographers named Whitfield (Whit) Diffie and Martin (Marty) Hellman revolutionized the world of

cryptography with the discovery of public key cryptography.[66] 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 encode the message, the recipient could 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.[67] For a military organization, it might be possible to protect that distribution, assuming no slipups 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

---

[66] 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 Levy, *Crypto*, 313-330. See also Levy, "The Open Secret," *Wired,* April 1999, http://www.wired.com/wired/archive/7.04/crypto.html (accessed January 21, 2008) and Singh, *The Code Book.*

[67] 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.

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.[68] 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.

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."[69]

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

[68] 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.
[69] Levy, *Crypto*, 89.

key) was essentially an algorithm that could 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.[70]

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 (a number) 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 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.

Section 3. Interactions with Congress, Other Government Agencies, and the Public

The next several sections discuss the NSA's political relationships with Congress and other federal agencies, as well as the troubled beginning of the NSA's engagement with the cryptographic community outside its walls and the first whiff of the legal challenges the export control regime would face. The discussion of the earlier period helps establish a baseline of behavior that shows how much the NSA's behavior changed and evolved in pursuit of its goal of

[70] 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.

slowing and limiting the use of encryption in later years. For the first few decades of its existence, the NSA's relationships with Congress were limited but cordial, while it fought repeated turf wars with the NSF over the exclusive right to fund and control cryptographic research. The agency's troubled relationship with outside cryptographers, mostly academics, slowly shifted from outright hostility (or a desire to silence) to an uneasy truce for the purposes of monitoring rather than suppression. Examples include the Meyer Letter and the secrecy orders the NSA attempted to place on various inventions and papers.[71] Later sections discuss the NSA's gradual shift away from total secrecy and the beginning of its attempts to reach out and engage with the cryptographic community outside its walls. Although these early attempts were largely unsuccessful, they reflect a willingness to adapt and work against organizational norms not always found in large organizations. Throughout the period discussed in this section, up through the early 1980s, the tension between the NSA's traditional desire to suppress and control cryptography, and to do so secretly, and its newer approach of managing and monitoring and engagement is clear. The agency swings back and forth, sometimes reaching out, often reverting back to old habits, but the overall trajectory moves toward a less strict approach.

NSA and Congress

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 as a primary interest, meshed neatly with the values of Congress during the Cold War. In addition, NSA had become very good at converting Congressmen to its cause:

[71] Obviously there is some selection bias here – only unsuccessful attempts to place secrecy orders can be documented.

> 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."[72]

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, a pattern that would continue into the 1990s. 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. In a disturbing parallel to the current investigations into NSA's warrantless wiretapping, the Committee discovered an effort called Project Shamrock that also 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.[73] Unfortunately, the timing of the RSA paper and Gardner's article did not help this plan. The promise of RSA was that universal private communications were indeed possible, exactly what the NSA feared. Its efforts to prevent this from happening therefore continued.

Turf Wars: NSF Round 1

The NSA fought hard to keep cryptography within its walls. Its efforts extended not only to the independent researchers and academics but to the agency that was its chief rival in funding

---

[72] Levy, *Crypto*, 264.

[73] Bamford, *Puzzle Palace;* Levy, *Crypto*, 106; Nicholas Horrock, "National Security Agency Reported Eavesdropping on Most Private Cables," *The New York Times*, August 8, 1975, 1. See especially United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans,* Final Report, Book II, April 26, 1976, and U.S.S., *Hearings on The National Security Agency and Fourth Amendment Rights*, Book 5, October 29 and November 6, 1975, http://www.aarclibrary.org/publib/church/reports/contents.htm. (accessed January 6, 2008). (Hereafter, "Church Committee Reports" and Book or Volume Number).

(and thereby controlling) cryptographic research, the NSF. The NSF is 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 the 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, and again the NSA could provide no documentation. 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…"[74]

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 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

[74] See account in U.S. House of Representatives, Committee on Government Operations, Government Information, and Individual Rights Subcommittee, *The Government's Classification of Private Ideas,* 96th Cong., 2nd sess., 1980. See also generally Bamford, *Puzzle Palace,* and Diffie, Landau and Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," *Science* 97 (July 29, 1977): 438-40; 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.

ability to easily and effectively perform its mission of reading SIGINT). Therefore, further attempts by the NSA to suppress and manage 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".[75] 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 had any involvement in the letter, it aroused deep suspicions as to NSA's intentions to restrict independent cryptographic research. Later investigations showed 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

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

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 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, backed 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.[76]

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.[77]

Secrecy Orders

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

[76] Levy, *Crypto*, 113.
[77] *Ibid.* 114.

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 scientists led 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, and 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.[78] Thus again, as with the Congressional investigations in 1975, it took a perceived crisis to force other branches of the government to act and force the NSA to back down.

Turf Wars: NSF, Round 2

By late 1977, Admiral Bobby Inman, who had taken over the directorship of the NSA only a few months ago, 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 defuse the anger and growing perception that the NSA was trying to restrict cryptographic research by actively impounding it and by luring researchers under NSA's jurisdiction, where their findings could be classified. His university tour did not meet with a warm reception, though it did

---

[78] *Ibid.* 116-7. For notes on Davida case, see Deborah Shapley, "DOD Vacillates on Wisconsin Cryptography Work," *Science* 201 (July 14, 1978): 141; Louis Kruh, "Cryptology and the Law–VII," *Cryptologia* 10 (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* 201 (September 8, 1978): 891-94; Bamford, *Puzzle Palace,* 446-51.

illustrate the NSA's growing recognition of and adaptation to the changes in the cryptographic world outside.

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 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.[79] 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.

First Amendment Problems

Despite these public setbacks, Inman still believed that the NSA had the upper hand because of ITAR regulations. He believed that export controls were the key to controlling cryptography, the only thing preventing a "disastrous free-for-all in the distribution of cryptography—the equivalent of a national security meltdown."[80] 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 could provide a 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

[79] Levy, *Crypto,* 118.
[80] *Ibid.* 119.

the NSF. Thus, "those regulations would become the linchpin of the agency's efforts to stop worldwide communications from becoming ciphertext."[81] 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.*[82]

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?*[83]

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

---

[81] *Ibid.* 119.
[82] 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 Lance Hoffman, *Building in Big Brother* (New York : Springer-Verlag, 1995).
[83] Levy, *Crypto,* 119.

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 tactics yet again.[84]

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 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.[85]

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

---

[84] See text of ITAR at http://epic.org/crypto/export_controls/itar.html (accessed January 21, 2008).
[85] Speech reprinted as Bobby Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," in *Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance,* eds. David Banisar and Bruce Schneier, 347 (New York: Wiley and Sons, 1997).

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]."[86] 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.[87] 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 submission.[88]

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 do.[89] 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

---

[86] Dissent reprinted as Davida, "The Case Against Restraints on Non-governmental Research in Cryptography," *Cryptologia* 5 (July 1981): 143.

[87] 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.

[88] Susan Landau, "Zero Knowledge and the Department of the Defense," *Notices of the American Mathematical Society (Special Article Series)* 35 (1988): 12, cited in Diffie and Landau, *Privacy,* 254.

[89] 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. Further explanation of the knapsack algorithm can be found at http://en.wikipedia.org/wiki/Merkle-Hellman and http://www.math.ucsd.edu/~crypto/Projects/JenniferBakker/Math187/index.html.

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.[90]

Section 4. Mass Market Cryptograhy: A New Wrinkle

Turning to the commercial sector, the early 1980s marked the beginning of mass market cryptography. The popularity of the personal computer created demand for commercial software, which inevitably led to the demand for secure communications – and therefore encryption software (or software with built-in encryption). From the NSA's perspective, it was a disaster waiting to happen: all of a sudden, the ability to encrypt communications would no longer be limited to the government, military, limited approved agencies and the occasional computer geek. It would be available to anyone, no technical expertise required, which meant an exponential increase in encrypted traffic—in other words, a lot more work for the NSA. Clearly, from an organizational interest standpoint, something needed to be done. What eventually happened bears resemblance to the DES story, in that the NSA used the review process for export to intervene in the development of commercial products, forcing changes in the algorithms used and cutting encryption key length. However, this time the product was released for mass market use, despite the NSA's misgivings. The mass market tidal wave was clearly on the horizon.

[90] John Markoff, "Paper on Codes is Sent Despite U.S. Objections," *New York Times,* August 9, 1989, http://query.nytimes.com/gst/fullpage.html?res=950DE5DD103BF93AA3575BC0A96F948260 (accessed January 21, 2008).

Lotus Notes

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.[91] 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 network) 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 both 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 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). When Ray Ozzie, the inventor of Notes, went down to Fort Meade to meet with the NSA about the export regulations in mid-1986, the effort immediately hit a stalemate.

With international sales making up over half of potential revenue, restricting sales to the U.S. domestic market only was not an option for Lotus, which depended on 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

[91] Chip manufacturing technology simply wasn't up to putting such complicated algorithms on so small a space yet.

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.[92]

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.[93] 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 version? – did not begin until a few years later, when the novelty of having a mass-market program with built-in encryption at all 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 terms of the Computer Security Act—see discussion in next section), and one with weaker 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

---

[92] Levy, *Crypto,* 159.

[93] *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).

influence on the government), they would help Lotus fight for stronger encryption and longer key lengths.[94] 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.

A few years later, faced with a similar problem, Microsoft would opt for ease of manufacturing and distribute a single, weaker (40-bit) version of its products, which Ray Ozzie dubbed "espionage enabled encryption".[95] 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.[96] However, the fact remained that the software was immensely popular, and built-in encryption in the public sector was here to stay.

---

[94] *Ibid.* 163-4.

[95] *Ibid.* 262.

[96] 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. Account from Levy, *Crypto,* 175-6.

Section 5. More Politics, Turf Wars, and Encryption Standards

The emergence of mass market software that contained encryption opened another front in the NSA's war to control cryptography. Clearly the civilian, mass market sector showed signs of becoming a very large problem, and as a result, the NSA renewed its attempts to obtain jurisdiction over civilian cryptography. A series of actions, most notably the Poindexter Directive and a rather ingenious circumvention of the Computer Security Act of 1987, represent this effort. Meanwhile, while export control provided an adequate, if not entirely satisfactory, weapon against software manufacturers, the NSA still faced the problem of the growing popularity of the already-approved DES algorithm, and the enormously popular (and strong) RSA algorithm. Having learned from the DES experience that not submitting an entry for the federal encryption standard led to reduced control over the final product, the NSA sought to remedy the problem by substituting a new, more satisfactory cryptographic system, the Commercial COMSEC Endorsement Program. Although the CCEP effort proved ultimately unsuccessful, the NSA found greater success with its proposal for the Digital Signature Standard (DSS). It was during the political maneuverings of the Computer Security Act and DSS that the NSA began to show the first signs of a new, and quite effective, tactic of recruiting law enforcement, particularly the FBI, as a political ally. The cooperation between the NSA and FBI and law enforcement agencies would achieve great significance in just a few years, with the introduction of the Clipper Chip.

CCEP: An Attempt to Replace DES

By the mid-1980s, NSA had come to regret its decision not to submit an algorithm in response to NBS's 1973 request for an encryption standard. DES had become unexpectedly popular, and as 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."[97] NSA's rationale was that widespread use of DES could prompt a hostile

[97] Ellen Raber and Michael O. Riley, "Protective Coatings for Secure Integrated Circuits," *Energy and Technology Review* (May-June 1989): 13-20, cited in Diffie and Landau, *Privacy,* 64.

intelligence organization to mount an attack on the cipher, which ironically had been weakened earlier by NSA's insistence on cutting the key length.[98] 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.

The 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 $1,000 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."[99] 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, 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.[100]

---

[98] Bob Davis, "A Supersecret Agency Finds Selling Secrecy to Others Isn't Easy," *Wall Street Journal,* March 28, 1988, 1.

[99] *Ibid.*

[100] The account of the CCEP program in this paragraph is taken from Diffie and Landau. The quote about the NSA sales pitch is from Cheryl Helsing, Chair, Data Security Committee, American Bankers Association, and VP for Corporate Preparedness and Information Security, Bank of America, Testimony in United States House of

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.[101]

NSDD-145 and the Poindexter Directive

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. Heavily influenced by the NSA, it gave the NSA control over all government computer systems containing "sensitive but unclassified" information.[102] Reagan justified the directive by noting that information is like a mosaic: while bits of unclassified are by themselves innocuous, in the aggregate they can reveal highly classified and sensitive information.[103] The Directive was followed by a second directive issued by National Security Advisor John Poindexter, which extended the NSA's authority to include non-government computer systems. 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.[104] A House of Representatives investigation ensued, and a turf battle

---

Representatives, Committee on Government Operations, Subcommittee, *Computer Security Act of 1987,* Hearings on H.R. 145, February 25, 26, and March 17, 1987, 100th Cong., 1st sess., 1987, 113-114.

[101] Type I equipment is managed through COMSEC accounts, which are generally 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.

[102] Clinton C. Brooks, Memo, April 28, 1992, reprinted in Banisar and Schneier, *Electronic Privacy Papers,* C8-C13; "Computer Security Act of 1987," http://epic.org/crypto/csa/ (accessed January 9, 2008).

[103] Robert Pear, "Washington Feeling Insecure About Non-Secret Information," *New York Times,* August 30, 1987, http://query.nytimes.com/gst/fullpage.html?res=9B0DEEDE1138F933A0575BC0A961948260&sec=&spon=&page wanted=all (accessed December 15, 2007).

It is worth noting that Reagan's justification was technologically accurate. It has become more so as more of our lives are lived electronically (thereby generating more data points) and computers have become more powerful (the better to sift through the data). Data mining, which has been the subject of much controversy since 2006, is based upon the principle of sorting through large quantities of data to extract relevant information. It has developed into one of the most powerful ways of gathering information, since many small bits of data can be compiled to generate a much larger and more complete picture.

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

between the executive and legislative branches began. Congress viewed the directives as an attempt to change national policy without consulting Congress. The Poindexter Directive was withdrawn soon after Congressional hearings began.[105]

Turf Wars: Computer Security Act of 1987

The hearings over NSDD-145 resulted in yet another piece of legislation, the Computer Security Act (CSA) of 1987.[106] 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.[107] 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.[108] 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."[109] 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

---

[105] 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 (USHR, *Hearings on HR 145,* 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 account from the notes to pg. 68 in Diffie and Landau, *Privacy,* and references Frank Carlucci, Letter to Chairman Jack Brooks, March 12, 1987, in USHR, *Hearings on HR 145,* 386.

[106] Computer Security Act of 1987, Public Law 100-235, 40 U.S.C. 1441.

[107] William Odom, Testimony in USHR, *Hearings on HR 145,* 294-5.

[108] 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., 26.

[109] *Ibid.* 21.

standards program with little say about most of the program – the technical standards developed by NSA. This would jeopardize the entire Federal Standards program."[110]

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[111]

The NSA soon found a way to maneuver around this setback. 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.[112] The Congressional Budget Office (CBO) estimated of the cost of implementation of the Computer Security Act ranged from $4-5 million per year.[113] 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 mandating that NIST "request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques."[114] A Technical Working Group (TWG)

---

[110] *Ibid.* 26.
[111] Brooks, Memo, C8-C13.
[112] United States Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, 1994, 164.
[113] USHR, Part 2, *Report on CSA,* 43
[114] 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.

was set up, with three members each from the NSA and NIST, which would review and analyze issues of interest prior to public disclosure.[115] 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."[116] 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."[117] In fact, the only person outside 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.)

Digital Signature Standard

Having learned from its experience with DES and the failure of the CCEP, the NSA began the process of developing a Digital Signature Standard with its usual technical skill and considerably more political acumen. 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.

---

[115] *Ibid.* 3.
[116] Milton Socolar, Testimony of, in United States House of Representatives, Committee on 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.
[117] United States Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* OTA-CIT-310, 1987, 164.

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.[118] 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."[119]

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.[120]

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[121]
- for signature verification, it was roughly 10 times slower to use than RSA on comparable processors (though 25 times faster for the actual signing)[122]
- the key could be used for signing only, not encryption[123]

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

---

[118] United States General Accounting Office, *Communications Privacy: Federal Policy and Actions,* (Letter Report, April 8, 1997, GAO/AIMD-97-49), 20, cited in Diffie and Landau, *Privacy,* 72.
[119] Private conversation between Landau and McNulty, cited in Diffie and Landau, *Privacy,* 72.
[120] 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* (Upland, PA: Diane Publishing Co., 1993).
[121] Brian LaMacchia and Andrew Odlyzko, "Computation of Discrete Logarithms in Prime Fields," *Design, Codes, and Cryptography* 1 (1991): 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, *Privacy*, 73.
[122] 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.
[123] Levy, *Crypto*, 178.

adopt the standard.[124] 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.[125] 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]."[126] 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.[127]

The Congressional hearings on the digital signature standard focused on the continued tension between the NSA and NIST, and on which agency should be in charge of the government's computer standards program.[128] 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."[129] 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 House report

---

[124] 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.
[125] John Lyons, Testimony in United States House of Representatives, 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., 1992, 163-176.
[126] United States Department of Commerce, National Institute of Standards and Technology, "Memorandum for the Record, January 31, 1990," reprinted in Banisar and Rotenberg, *1993 Sourcebook.*
[127] Levy, *Crypto,* 184.
[128] United States Department of Commerce, National Institute for Standards and Technology, "Memorandum for the Record, March 26, 1990," in Banisar and Rotenberg, *1993 CPSR,* 19.
[129] USHR, Part 2, *Report on CSA,* 19.

accompanying the legislation."[130] GAO's evaluation stated: "NIST follows NSA's lead in developing certain cryptographic standards."[131] 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.[132] After some effort, the NSA convinced the FBI that encryption was indeed an important and critical issue that threatened the FBI's treasured wiretapping abilities. The FBI came to be an invaluable ally in the coming years. An NSA-NIST-FBI interagency group formed, but with 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 that would be palatable to the American public, and by extension to Congress—namely, law enforcement.[133] 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.

Section 6. 1991: A New Era with New Challenges

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

[130] USC-OTA, *Information Security*, 13-14.
[131] United States General Accounting Office, *Communications Privacy: Federal Policy and Actions*, GAO/OSI-92-2-3, November 1993, in Levy, *Crypto*, 183.
[132] Private conversation between Landau and Kammer, January 17, 1997, in Diffie and Landau, *Privacy,* 75.
[133] Diffie and Landau, *Privacy,* 76.

phone lines and optical cables also fueled the push toward greater access toward cryptography. The introduction of 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. 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, cryptography would break free of most of its government-imposed fetters.

For the NSA, the 1990s marked a decade when the strategy undeniably shifted toward slowing the spread of cryptography, and most likely, privately building up and solidifying its technical advantages while publicly attempting to implement escrowed encryption. Although most of the action seems to take place in the political arena, with the FBI and other key political allies pushing key escrow as a solution that would allow users to have their encryption without compromising law enforcement's ability to protect the public, it seems likely that the agency itself recognized that where the battle was most likely to be won was on the technological battlefield, secretly building up capabilities behind the Triple Fence, funding research into mathematics and quantum computing and other fields. In this sense, allowing the FBI and others to take the initiative in the highly public and political debate over Digital Telephony and the Clipper Chip allowed the NSA to retreat and concentrate on its traditional (technological) strengths.

Despite the ultimate failure of the Escrowed Encryption Initiative, it served to delay by several years the loosening of export controls and very likely the development of other encryption alternatives (in the sense that the looming adoption of the NSA-approved standard would discourage competitors from developing alternatives that would languish on the market without the backing of the government.) In this sense, the 'failure' to adopt the Clipper Chip was still a victory for the NSA, although it is not clear that the FBI and other law enforcement, which

lacked the NSA's 'last resort' ability to secretly gather and decrypt communications through brute computing capabilities, understood this.

Pretty Good Privacy (PGP)

PGP represented 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, not only marked the end of real effectiveness for export controls, it also forced the NSA to seek alternative means of managing encryption software, an effort that culminated in the ultimately successful passage of the Communications Assistance for Law Enforcement Act and the unsuccessful attempt to implement the Escrowed Encryption Initiative (better known as the 'Clipper Chip').

PGP was the brainchild of Phil Zimmermann, a computer programmer and privacy activist who feared that electronic surveillance would provide the government with a powerful tool for monitoring dissent. 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, and encryption for everyone, he believed, was the answer to the dilemma. He began developing PGP in 1984, designing it to be compatible with the slower processor speeds of personal computers, which could not easily handle the bulky algorithms public key encryption required. Instead, he substituted a hybrid system of RSA key

exchange protocols[134] and a faster encryption algorithm written by fellow cryptography enthusiast Charlie Merritt.[135] The end result was a program that ran on many different types of processors, was (relatively) easy to use, and easily copied and circulated. In other words, it was an NSA nightmare.

Meanwhile, the FBI, newly aware of the dangers of cryptography, was hard at work trying to preserve its wiretap capabilities. On January 24, 1991, at the explicit request of the FBI, Sen. Joseph Biden, the chairman of the Senate Judiciary Committee, inserted a clause into a pending piece of anti-terrorism legislation known as Senate Bill 266. The clause read:

---

[134] The use of RSA protocols later created legal problems for Zimmermann, who had chosen RSA based on its effectiveness and without much thought to licensing. 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. 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 downloaded, on the honor system. Frustrated, he decided to ignore the problem and go back to finishing PGP. (See Levy, *Crypto,* 193).

When PGP was originally 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.

The patent dispute was finally resolved in 1994, 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.

[135] 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.

> *"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."*[136]

The implications of the sentence, which initially escaped scrutiny in the massive bill, were devastating for the cryptographic revolution. The point of encryption, and 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. It was the first step toward 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."[137] 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 he later told the *Micro Times,* a San Francisco-based computer-oriented newspaper, "The intent here is to invalidate the so-called trapdoor provision of the new Senate bill coming down the pike before it makes it into law."[138] Zimmermann abandoned his original plan to distribute PGP as shareware and distribute it as freeware over the Internet. In 1991, the Internet was still largely the domain of the computer savvy—precisely those who because of technological skill and ideology would respond to the program.[139]

The story of how PGP was actually released is somewhat comical: one of Zimmermann's friends, Kelly Goen, who had clearly watched too many spy movies, drove 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

---

[136] "Comprehensive Counter-Terrorism Act of 1991," 102nd Cong., 1st sess., 1991, S. 266, http://thomas.loc.gov/cgi-bin/query/D?c102:3:./temp/~c102Yj9F8N:: (accessed January 21, 2008).
[137] Jim Warren, "Is Phil Zimmermann Being Persecuted? Why? By Whom? Who's Next?" *Micro Times*, April 1995.
[138] *Ibid.*
[139] 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.

many copies scattered as widely as possible around the nation before the government could get an injunction and stop him."[140] 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."[141]

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.

PGP 1.0 met with an enthusiastic reception from cryptography enthusiasts around the world, who set about improving and strengthening the program. At Crypto '91, a cryptography conference, Zimmermann met a NSA mathematician named Brian Snow and a colleague of Adi Shamir's named Eli Biham, who informed him that the encryption algorithm used in PGP was weak, i.e., vulnerable to a differential cryptanalysis attack, the T attack that IBM researchers had discovered in their development of DES more than a decade ago. Thus for PGP 2.0, Zimmerman and a group of volunteers substituted in a new encryption algorithm, the Swiss 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

[140] Levy, *Crypto,* 196.
[141] *Ibid.* 198.

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.[142]

The popularity of PGP brought legal troubles for Zimmermann: the Department of Justice (DOJ) began investigating him for violation of export control regulations for posting PGP on the Internet. After the 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. In addition, Zimmermann had not actually posted the code himself; Goen had done that, and he had limited himself to posting to sites within the U.S.. And perhaps most importantly from a public relations standpoint, the Massachusetts Institute of Technology (MIT) had gotten involved in the distribution of PGP, hosting it on its servers.

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.[143] 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.[144] 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

---

[142] *Ibid.* 203.

[143] Thomas E. Weber, "Should Only the Paranoid Get E-Mail Protection?--Probably Not, As `Encryption' Gets Easier," *The Wall Street Journal*, September 25, 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,* April 28, 1994, A1; Levy, *Crypto,* 289.

[144] 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.

prosecution, if not the displeasure of the NSA.[145] 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.[146] 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 old as NSA, just as well funded, and even more influential in the military-industrial complex. The Department of Justice let the case drop."[147]

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."[148]

The release of PGP, and its near instant spread over the Internet and thereby international borders, demonstrated just how far cryptography outside of NSA's wall had come. It also showed how quickly, and with how little control, encryption software could spread. Once PGP was released, there was nothing the NSA or its political allies could do about it – which meant that even if it hadn't before, the NSA needed to shift strategies from trying to suppress civilian cryptography to either replacing it with something more palatable, or more likely, to building up and consolidating as much of a technological advantage as possible.

---

[145] NSA's displeasure was probably justified: MIT versions of PGP were spotted outside the country within two days of the first upload.
[146] OCR fonts can be readily scanned and converted into code with a personal scanner, available at any computer supply store for less than $100.
[147] Diffie and Landau, *Privacy,* 206.
[148] Levy, *Crypto,* 204.

However, the first task would prove extremely difficult. Too many actors with an interest in the free reign of cryptography had emerged since the 1970s. Cryptography was no longer an NSA monopoly, nor the realm of a few academics and tinkers. Software manufacturers and technologically savvy civil liberties groups, each with economic and ideological reasons for opposing controls on cryptography, had begun to realize what was at stake and fought to preserve their right to create, sell, and use strong encryption. The civil liberties activists, in particular, couched their argument not in terms of a right to encryption, but in terms of First Amendment rights to expression – to write (and use) code as a form of protected speech.

Crypto Anarchy and the Cypherpunks

The cause of free speech through cryptography brought together a diverse but ultimately effective coalition of cryptographers, civil libertarians, academics, geeks, paranoiacs, eccentrics, and the software industry, each of which had a stake in keeping strong cryptography strong and widely available. One organization that emerged during this period was the Electronic Frontier Foundation (EFF), a group dedicated to preserving civil liberties against digital and electronic encroachment. The group was founded by John Gilmore, who had been Employee No. 5 at Sun Microsystems before cashing out in 1986, Mitch Kapor, of Lotus Notes fame, and John Perry Barlow, the Grateful Dead's lyricist. Gilmore's hobby was making sure that information about cryptography 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.) As a result, he–and now the EFF–file many Freedom of Information Act (FOIA) requests.

Often the EFF's efforts were directed at exposing the inconsistencies in the government's cryptography policy. In one incident, Gilmore filed FOIA requests to declassify four early cryptanalysis texts by NSA cryptanalyst William Friedman. When the government failed to respond within the specified legal time period, he hired a lawyer to sue the government. In the course of the suit, he discovered that the texts had been declassified, then re-classified in the Reagan era. However, 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 initially told 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, even though technically Gilmore had only checked out a book from a public library and shared 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. Oddly enough, the other, identical copies remained classified.

Meanwhile, Eric Hughes and Tim May, two anti-government mathematicians in California, organized 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 cryptoanarchy. 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 soon became one of the most thorough, complete, and effective means to track not developments in cryptography, both technical and political. Thus, a few interested individuals, facilitated by the Internet, created 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*.

Section 7. A National Encryption Policy

New Political Allies, A New Approach

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.[149] 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 have a carefully controlled means of being able to decrypt information when legally authorized to do so," thus marking a 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.[150] 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.[151] 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

---

[149] Brooks, Memo, C8-C13.
[150] *Ibid.* C12.
[151] 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, reprinted in Electronic Privacy Information Center, *1995 EPIC Cryptography and Privacy Sourcebook: Documents on Wiretapping, Cryptography, the Clipper Chip, Key Escrow and Export Controls* (Upland, PA: Diane Publishing Co., 1995), C14, cited in Diffie and Landau, *Privacy,* 207.

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.

Although the rather late realization that they would need to seek political allies other than just the two Congressional intelligence committees shows a degree of political naïveté, the contrasting reaction of the law enforcement agencies (LEAs) also shows just how important the NSA's deep understanding of encryption was. Their technical understanding allowed them a degree of foresight – of understanding of potential consequences of a technology that had not yet fully developed nor deployed – that other agencies lacking this knowledge could not achieve.

After the NSA brought the FBI and DOJ into the anti-cryptography 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.[152] 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. Thus much of the government action during the 1990s features the FBI, rather than the NSA – a deliberate step back, possibly to focus on building and solidifying their pre-existing technical advantage, rather than attempting to win the cryptographic battle through political means.

The one exception to the anti-publicity policy of the NSA was Clinton Brooks, the Assistant to the Director. Brooks *wanted* a national debate on cryptography and key escrow,

---

[152] Levy, *Crypto* 240.

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.[153] 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 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.[154] 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

---

[153] The Clipper Chip is a two-part encryption system. When a Clipper Chip begins encrypting a message, it first sends out a signal called the Law Enforcement Access Field (LEAF). The LEAF is linked to the encryption key used, so both must match for a message to be decrypted. The LEAF can only be decrypted by a special government-held key unique to that particular chip (the first half of the escrowed key). Decrypting the LEAF reveals the identity of the unique Clipper Chip and its associated encryption key (the other half of the escrowed key). Both the LEAF and its associated encryption key are required to decrypt a message.

[154] Diffie and Landau, *Privacy*, 208.

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, however, was to set the course for the NSA-FBI lobbying – and eventual capture – of the new Clinton administration.[155]

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.[156] 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.[157] 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. 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."[158] The FBI's explanation of the contradiction was that *anticipated* technological problems had kept them from seeking or executing court ordered wiretaps. FOIA

---

[155] Levy, *Crypto,* 231.
[156] Advanced Telephony Unit, Federal Bureau of Investigation, "Telecommunications Overview" briefing, 1992, cited in Diffie and Landau, *Privacy,* 183.
[157] FBI. "Digital Telephony Proposal," reprinted in CPSR, *1993 Sourcebook.*
[158] John Mintz, "Intelligence Community in Breach with Business," *Washington Post,* April 30, 1992, A8.

litigation filed by the Computer Professionals for Social Responsibility, however, could not find a single example of wiretapping being foiled by technology.[159]

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.[160] Congress, too, rejected the bill, with no one 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.[161] The General Services Administration described the proposal as unnecessary and potentially harmful to the nation's competitiveness.[162] 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."[163] Apparently, the FBI did not think the measure would pass when it was submitted, either; their internal memoranda showed a 30% chance.[164]

In addition, it was an election year, and such controversial and complicated issues were politically inconvenient during the election year. Brooks figured that George H.W. Bush's 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,

---

[159] Diffie and Landau, *Privacy,* 184.

[160] 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, 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., 1994, 53-64, and United States House of Representatives, Committee on the Judiciary, *Report on Telecommunications Carrier Assistance to the Government,* HR 103-827, 103rd Cong., 2nd sess., 1994, 53-64.

[161] United States General Accounting Office, *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.

[162] United States General Services Administration, "Attachment to May 5, 1992 GSA memo, p.2," in CPSR, *1993 Sourcebook,* in Diffie and Landau, *Privacy,* 184.

[163] National Telecommunications and Information Agency, "Technological Competitiveness and Policy Concerns," 1992, in Electronic Privacy Information Center, David Banisar, ed., *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls* (Upland, PA: Diane Publishing Co., 1994).

[164] Lynn McNulty, Memo for the Record, August 18, 1992, in Electronic Privacy Information Center, *1996 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls* (Upland, PA: Diane Publishing Co., 1996), C14-C19.

two minor problems came up: first, the introduction of the TSD3600. Secondly, Bush lost.[165] 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 encryption chips? Sessions offered several inducements: first, that AT&T could claim that it was providing stronger encryption, since the Skipjack algorithm in the Clipper Chip was more powerful and difficult to crack than DES. Second, the U.S. would probably allow export of the escrowed phone, thereby considerably increasing the potential market. 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.[166] 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

[165] Levy, *Crypto*, 235.
[166] *Ibid.* 238.

DES algorithm instead in fall 1992. AT&T promised the NSA-chip version would soon join the product lineup.[167]

The Clinton Administration and Clipper

The tides were turning against the NSA and LEAs in terms of the public's view of cryptography and the forces allied against restrictions. The NSA's Stewart Baker realized that the government needed another solution. They could not mandate what people in the U.S. could use; they could not keep PGP away from anyone with a computer and an Internet connection. Realistically, most people would not go through the bother of finding programs like PGP and learning how to use them, but for those who wanted it, the government could not stop them. Export controls could keep strong cryptography away from the bad guys on a mass scale, but Congressional support for export controls seemed to be waning. Moreover, as with determined individuals in the U.S., there was little the NSA or LEAs could do about a foreign national determined to get his hands on strong encryption.

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 and LEAs 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.[168]

The NSA and FBI set about convincing the new Clinton administration of the necessity of key escrow even before they in Washington, and they were quite successful. FBI Director

---

[167] *Ibid.* 237; Diffie and Landau, *Privacy,* 208 for account of inserting escrowed chips into TSD3600.
[168] Levy, *Crypto*, 241-2.

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.[169] After these two unpleasant options, the law enforcement-national security coalition would present the Clipper chip option, which sounded quite reasonable by comparison.[170]

The national security-LEA 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 on 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 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

---

[169] *Ibid.* 243-4.

[170] 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. From Levy, *Crypto*, 245.

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 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, 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.[171]

Barely three months after taking office, on April 16, 1993, the Clinton White House announced the Escrowed Encryption Initiative, a federal standard that was intended to "improve security and privacy of telephone communications."[172] 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.[173] (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 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 NSA.)[174]

---

[171] *Ibid.* 246-7.
[172] NIST, "NIST Announces Voluntary Escrowed Encryption Standard to Promote Secure Telecommunications," http://www.nist.gov/public_affairs/releases/n94-08.htm (accessed February 1, 2008).
[173] The operation of the Clipper chip reflected this split duplicate key.
[174] Levy, *Crypto,* 232.

The proposed standard would be limited to encryption of voice, fax, and computer information transmitted over a telephone system.[175] Of course, this could be read to include almost all activity on the Internet as well as e-mail transmissions, since during this period of dial-up connections *everything* ran over the telephone system. 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 right to unbreakable commercial encryption.[176] The administration would later state that it would not seek legislation limiting the use of encryption.[177]

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.[178] 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."[179] 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.[180]

---

[175] 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.
[176] The White House, Office of the Press Secretary, "Statement on the Clipper Chip Initiative," April 16, 1993, in EPIC, *1994 Sourcebook.*
[177] USDoC-NIST, "Escrowed Encryption Standard," 5998; John M. McConnell, Testimony in United States Senate, Committee on the Judiciary, Subcommittee on Technology and the Law, *Administration's Clipper Chip Key Escrow Encryption Program,* Hearings, May 3, 1994, 103rd Cong., 2nd sess., 1994, 102, in Diffie and Landau, *Privacy*, 211.
[178] Steven Levy, "The Cypherpunks vs. Uncle Sam," *Sunday New York Times Magazine,* June 12, 1994.
[179] Diffie and Landau, *Privacy*, 212 and footnotes.
[180] Philip Elmer-Dewitt, "Who Should Keep the Keys?" *Time,* March 14, 1994, cited in Levy, *Crypto,* 261.

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.[181] 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 necessarily because they were criminals; it was because they simply didn't trust the government.[182] To create a system where the very government they were trying to encrypt their communications against held the escrowed key 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.

---

[181] *Ibid.* 251.
[182] *Ibid.* 252.

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.[183]

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 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.[184] Unfortunately, Kallstrom had no answer to the question of what smart criminals – or people from other countries – might do as an alternative.

---

[183] Diffie and Landau, *Privacy*, 213.
[184] Levy, *Crypto*, 255.

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.[185] 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.[186]

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 (Law Enforcement Access Field, or LEAF). He used a card reader and a program that simulated a wiretap, and 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 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

[185] 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, *Privacy*, 214.
[186] Diffie and Landau, *Privacy*, 214.

did not object. Neither did his superiors at AT&T, even though they had millions of dollars riding on the Clipper phones.[187] John Markoff of the *New York Times* 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."[188] 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.[189] 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.[190]

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.[191] The NIST issued a list of ten principles for software key escrow, compliance with which would allow export. However, NIST had no role in the export approval

---

[187] 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.

[188] John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *New York Times,* June 2, 1994, A1. 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.

[189] 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, *Privacy*, 215.

[190] 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, in Diffie and Landau, *Privacy*, 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.

[191] Diffie and Landau, *Privacy*, 208.

process, and the Department of Commerce played only a limited role, secondary to the Department of State, which deferred to the NSA on encryption issues.[192] 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.[193] Eventually, the key length restrictions and interoperability requirements were dropped.

Digital Telephony, Round 2

The FBI's aggressive campaign to preserve the value of its wiretaps 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. [194]

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 confused electronic bugs with wiretaps (the former does not require involvement by telephone companies) in his speeches.[195] In April 1994, in response to criticisms that his examples were vague, Freeh submitted examples of 183 cases in

---

[192]Authority over the export approval process was transferred from the Department of State to the Department of Commerce in 1996.
[193] Diffie and Landau, *Privacy*, 216.
[194] Communications Assistance for Law Enforcement Act, Public Law 103-414, Section 109, 47 U.S.C. §1008.
[195] Louis Freeh, Speech to the Executives' Club of Chicago, February 17, 1994, and Louis Freeh, Testimony in USS and USHR, *Digital Telephony,* 5-51, cited in Diffie and Landau 195-6.

which the FBI had had difficulty executing court-ordered surveillance.[196] 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.[197] After some difficulty and much lobbying, Freeh convinced Congress to pass the bill that he had made his agency's highest priority.[198] It was called the Communications Assistance for Law Enforcement Act.[199]

Obviously, encryption significantly diminishes the value of a wiretap. 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.[200] 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.[201] 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.[202] 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."[203] The fact that the NSA, historically so protective of encroachment on its turf (cryptography), did not object suggests that the FBI may have acted with the tacit approval of the NSA. Certainly, the position the FBI advocated accorded neatly with NSA interests.

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,

---

[196] USS and USHR, *Digital Telephony,* 14.
[197] USS and USHR, *Digital Telephony,* 14-5.
[198] Sabra Chartrand, "Clinton Gets a Wiretapping Bill that Covers New Technologies," *New York Times,* October 9, 1994, A27, cited in Diffie and Landau 196.
[199] "To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other...," 103rd Cong., 2nd sess.., 1994, H.R. 4922.
[200] 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, 6, in EPIC, *1994 Sourcebook,* 1994.
[201] This reply to a question apparently took place during a conference on Global Cryptography in Washington, DC, in September 1994. Diffie and Landau, *Privacy*, 202.
[202] Louis Freeh, Statement to Committee on Commerce, Science, and Transportation, U.S. Senate, July 25, 1996.
[203] United States Department of Commerce, National Institute of Technology and Standards, "Public Key Status Report," in EPIC, *1996 Sourcebook,* C-3.

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."[204] The beachhead for a renewed attempt to gain access to encrypted communications 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 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. For the NSA, the shift into the courts represented another arena for the cryptography debate it probably had not anticipated. For the most part, the agency was silent throughout these proceedings.

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.[205] Bernstein's program transformed the hash function into something that could encrypt and decrypt.[206] Still, in the court's decision, it reasoned that source code was "language"

---

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

[205] A hash function can be thought of as a way to rearrange data. It turns data into a relatively small number that serves as a 'fingerprint' of the data by 'chopping and mixing,' hence "hash," (substituting and transposing) the data. See Wikipedia, "Hash Functions," http://en.wikipedia.org/wiki/Hash_function (accessed January 8, 2008) for more information.

[206] 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

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."[207] 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) 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."[208]

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 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."[209] 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 (AECA)

---

through customs without a trigger, and the new program as a kit that installs the missing part." See Levy, *Crypto,* 298.

[207] 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), cited in Kurt M. Saundersby, "The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff," 17 *John Marshall J. of Computer and Information Law* 945 (1999).

[208] *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," 13 *Berkeley Technological Law Journal* 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," 2 *Virginia J. of Law and Technology*. 3 (1997); Levy, *Crypto*, 300-2.

[209] 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.

and ITAR were unconstitutional under the First and Fifth Amendments.[210] 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."[211]

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 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

---

[210] *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, "Regulation." 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.

[211] Junger v. Daly, 8 F. Supp. 2d. 708 (N.D. Ohio 1998), in Saundersby, "Regulation." For more information on the case, see "Free Speech and the Export of Crypto," http://samsara.law.cwru.edu/comp_law/crypto_export (accessed August 2, 2004).

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 earlier – 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 Computer Science and Technology Board (CSTB) of the National Research Council (NRC) after the Clipper controversy.[212] 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."[213] 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

---

[212] 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.

[213] 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* (Washington, D.C.: National Academy Press, 1996), 298.

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.[214]

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 position, that "no law should bar the manufacture, sale, or use of any form of encryption within the United States."[215] To deal with the complications that encryption would present to law enforcement, the panel recommended that the government 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.[216] The CSTB report was not what the Clinton administration wanted to hear.

Section 8. 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 of 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.

The less technically inclined reader can skip this section and go to "Mr. Gates Goes to Washington".

---

[214] Diffie and Landau, *Privacy,* 300-1.
[215] *Ibid.* 303.
[216] *Ibid.* 299.

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 $100 to anyone who could factor the number (i.e., decrypt the published encrypted message) and predicted it would take forty quadrillion years to do so. With 39 quadrillion-plus years to go, Atkins decided to tackle the problem.[217,218] Back when Rivest, Shamir and Adleman had come up with the challenge, they had known that new and better factoring algorithms would 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 and 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.[219] 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 =
114381625757888867669235779976146612010218296721242362562561842935706935245733
89783059 712356395870505898907514759929002687954354 1
= 3490529510847650949147849619903 8 9813341776463849338784399082057 7 *
3276913299326670954996198819083 4 4614131776429679929425397982885 33.

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."

---

[217] 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.

[218] 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.

[219] For a full explanation, see "A Discussion of RSA-129 Activity," http://www.math.okstate.edu/~wrightd/numthry/rsa129.html (accessed February 3, 2008) for documentation on the breaking of RSA-129. For an explanation of the algorithm, see Eric Landquist, "The Quadratic Sieve Factoring Algorithm," December 14, 2001, http://www.math.uiuc.edu/~landquis/quadsieve.pdf (accessed February 3, 2008).

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.[220]

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 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

[220] 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.

RSA-129 crack, was Mr. Cosmic Kumquat, of SSL Trusters, Inc., 1234 Squeamish Ossifrage Road.[221]

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.[222] 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 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.[223]

---

[221] 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, 11.
[222] 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".
[223] Jonathan Gornall, "Netscape Plugs Latest Leak," *The Times,* September 27, 1995.

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.[224] 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 (EFF) funded a project by John Gilmore and Paul Kocher to build a DES-cracking machine. DES, of course, was still highly restricted. They spent about $210,000 building their machine, and at a 1998 cryptography conference, Gilmore and Kocher used it to produce the plaintext of a DES encrypted message in 24 hours. The implications of this cracking effort were obvious. If DES could be broken 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.)[225] 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 weak even restricted encryption schemes were, and therefore how little benefit to national security preventing their export provided. 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

[224] For discussion of both Netscape hack efforts, see Levy, *Crypto*, 278-283.
[225] Levy, *Crypto*, 302.

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

Software Lobby in 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. (Ozzie had been the principal creator of IBM's Lotus Notes.) 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 what one might think on the basis of past actions, banned from domestic surveillance.[226] Ozzie hoped that dangling the possibility of a NSA-specific key escrow scheme would split the NSA from the other government agencies that depended on its technical expertise as well as the White House, so that in the confusion, industry could sneak its own solution through.[227]

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 IBM, which had purchased Lotus a few years earlier, to penalties, including jail time. 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.[228]

Section 9. 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

---

[226] 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, *Privacy*, 146, for discussion of Nixon's illegal use of the NSA to monitor communications of U.S. citizens using international facilities.

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

[228] Ibid.

international efforts as well, since the export controls were ostensibly directed at controlling access to encryption in other countries. Seeking international cooperation to secure the export control regime was nothing new; it was simply an attempt to revive CoCom (Coordinating Committee for Multilateral Export Controls), which had been dissolved in 1994 and was later replaced by the Wassenaar Arrangement.

The Clinton administration quietly sent its representatives to lobby for tighter controls in other countries, but met with little success other than 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 represented).[229] 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]".[230] 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

[229] Diffie and Landau, *Privacy*, 220-1.

[230] *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* 30 (Spring 1999).

protocols for cryptographic methods... be market driven."[231] The U.S. was in the minority on this issue. The Scandinavian countries and The Netherlands all favored placing no limits on citizens' rights to use encryption, including strong cryptography without trap doors.[232] 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."[233]

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.[234] The Wassenaar members had placed encryption items on the original Dual-Use Control List, but had not determined a ceiling on the strength 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.[235] However, this

---

[231] OECD, "Cryptography Policy Guidelines," March 27, 1997, http://www.oecd.org/document/11/0,3343,en_2649_201185_1814731_1_1_1_1,00.html (accessed February 3, 2008).

[232] 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,* 4 (Spring 1996), 4-7; private conversation between Landau and Deborah Hurley, April 3, 1977, all cited in Diffie and Landau, *Privacy,* 221.

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

[234] Stewart A. Baker & Paul R. Hurst, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce 605* (The Hague: Kluwer Law International, 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," 15 *American University International Law Review* 271 (1999).

[235] F. Lynn McNulty, "Encryption's Importance to Economic and Infrastructure Security," *Duke Journal of Comparative and International Law,* Spring 1999, see n54. This note references www.wassenaar.org/list/cat5p2.pdf

change was largely illusory, as the Wassenaar Arrangement is a non-binding regime.[236] The U.S. policies on encryption restriction were the strictest among industrialized democracies at the time.[237] 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.[238] 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.[239] 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.[240] 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.[241] 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.

---

[236] Shehadeh, "Wassenaar." Although not completely meaningless, noncompliance with the regime by members rendered the actual effect of listing encryption over 64-bits rather minor.

[237] EPIC, *Cryptography and Liberty 1999: An International Survey of Encryption Policy* (Washington, D.C.: EPIC, 1999).

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

[239] Kenneth A. Dursht, "From Containment to Cooperation: Collective Action and the Wassenaar Arrangement," 19 *Cardozo Law Review* 3 (December 1997): 1079-1123.

[240] See Network Associates Products, "Total Network Security: Cryptographic Products," http://www.nai.com/products/security/tis<uscore>research/crypto/crypt<uscore>surv.asp (accessed February 22, 1999), cited in McNulty, "Encryption's Importance."

[241] "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 Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology Will Drive Policy," in *Borders in Cyberspace,* eds., Brian Kahin and Charles Nesson (Cambridge, MA: MIT Press, 1997), 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, in Levin, "Who are We Protecting?", note 47.

Section 10. The Beginning of Liberalization

Congress: Early 1990s

By the mid-1990s, the tides had turned against restriction of access to encryption. Government efforts to control encryption relied on two legs, key escrow 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 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.[242] 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 cryptography, even if they couldn't eliminate it completely.

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.[243] 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

---

[242] Levy, *Crypto,* 262.

[243] 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.

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.[244]

Congress had finally gotten back into the game. At the instigation of the new House Representative Maria Cantwell (D-Wash.) from eastern Seattle, a region that included a bevy of high tech companies including Microsoft and Nintendo, and Sam Gejdenson (D-Conn.), Chairman of the House Committee on Foreign Affairs, Subcommittee on Economic Policy, Trade, and Environment, hearings were held to draw 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."[245] 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."[246] While most of Congress still accepted the NSA's views, the gap between the NSA's public position 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 pointed out 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

---

[244] Levy, *Crypto,* 205.
[245] *Ibid.* 263.
[246] John Schwartz, "Bill Would Ease Curbs on Encoding Software Exports," *The Washington Post,* November 23, 1993, C1.

could.[247] 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 Rep. 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."[248]

Cantwell began preparing a bill (HR 3627, "Legislation to Amend the Export Administration Act of 1979") to fix the export control regime, at least with respect to encryption. It would move the decision making process out of State to Commerce, which would shift the rules regime from ITAR to EAR, which was a less restrictive set of rules. Although the NSA would still have a seat on the (technical) review committee, the chair of the committee would shift to Commerce, which could set the review process to further an agenda different from that of the State Department.[249] The legislation would also 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 cut off a Congressman's lecture on the importance of export controls and informed the committee members that the rules were nonsense.[250]

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.[251] Cantwell discussed the proposal with the industry group Business Software Alliance, and they

---

[247] 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 Cong., 1st sess., 1993, in Levy, *Crypto,* 265.

[248] *Ibid.*

[249] I thank Eugene Skolnikoff for pointing out the significance of shifting jurisdiction from the State Department to the Commerce Department, and thereby from ITAR to EAR (Export Administration Regulations).

[250] Levy, *Crypto,* 266.

[251] 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; John Markoff, "Gore Shifts Stance on Chip Code," *New York Times,* July 21, 1994, D1.

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. The White House promises had been intended to "placate Rep. Cantwell and avoid a national debate."[252] It had exactly the opposite effect. As it turns out, the White House had neglected to consult the NSA or the FBI before making those promises, showing that the national security-LEA alliance still held considerable sway in the Clinton administration. 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 began working on the issue 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.[253] 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.

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

---

[252] Levy, *Crypto*, 267.

[253] Associated Press, "Appeals Court: Rep. McDermott Violated law in Leaking Taped Call," March 28, 2006, http://www.foxnews.com/story/0,2933,189364,00.html (accessed January 12, 2008); Martin Halstuk, "Rights v. Privacy: A Pending Case May Open a Back Door to Prior Restraint," *Columbia Journalism Review,* 2003, http://cjrarchives.org/issues/2003/1/privacy-halstuk.asp (accessed January 15, 2008).

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.[254] 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.[255] 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.[256] 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 (key escrow) 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: Mid- to late-1990s

Congress had come a long way in the five years since Maria Cantwell's initial, failed 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

---

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

[255] 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 cited in Shehadeh, "Wassenaar."

[256] See 50 U.S.C. app. § 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.".

Electronic Privacy Information Center (EPIC, which engaged in a series of FOIA litigation 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 cryptography debate in the House included 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, as well as Patrick Leahy and Patty Murray ("the senator from Microsoft").[257] 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 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 harbinger of a 'digital Pearl Harbor'. Even the military got into the act, holding 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 cryptography lobby, was the very thing the government had been trying to suppress for a half a century: strong cryptography.

---

[257] Levy, *Crypto*, 304.

In March 1996, Sen. Patrick Leahy introduced the Encrypted Communications Privacy Act of 1996, 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.[258] A month later, Sen. Conrad Burns (R-Montana) introduced the Promotion of Commerce On-Line in the Digital Era (PRO-CODE) bill, which specifically prohibited mandatory key escrow, affirmed the right to sell and use any encryption domestically, and liberalized export controls.[259] Somewhat predictably, the bill was bottled up in congress, trapped by legislators heavily influenced by the NSA's briefings. In addition, it was an election year and therefore unsuitable for debate of complex legislation. Burns would re-introduce PRO-CODE in 1997.[260]

In 1997, Rep. Bob Goodlatte would introduce the Security and Freedom through Encryption (SAFE) Act.[261] 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 Department of Commerce and permitted export of strong encryption if similar product already existed 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 the Senate, the introduction of a piece of rival 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.[262] 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. 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

---

[258] "Encrypted Communications Privacy Act of 1996," 104th Cong., 2nd sess., 1996, S. 1587, http://thomas.loc.gov/cgi-bin/query/D?c104:5:./temp/~mdbsvk1SJt:: (accessed January 21, 2008).
[259] "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996," 104th Cong., 2nd sess., 1996, S. 1726, http://thomas.loc.gov/cgi-bin/query/D?c104:3:./temp/~mdbsvGqhA3:: (accessed January 21, 2008).
[260] "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997," 105th Cong., 1st sess., 1997, S. 377, http://thomas.loc.gov/cgi-bin/query/F?c105:3:./temp/~mdbsEUhuIG:e0: (accessed January 21, 2008).
[261] "Security and Freedom Through Encryption (SAFE) Act," 105th Cong., 1st sess., 1997, H.R. 695, http://thomas.loc.gov/cgi-bin/query/C?c105:./temp/~c105fX0hvz (accessed January 21, 2008).
[262] "Secure Public Networks Act," 105th Cong., 2nd sess., 1998, S. 909, http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~mdbsQJy4Eo:: (access January 21, 2008).

House National Security Committee, Reps. Porter Goss and Norman Dicks 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.[263]

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 in 1999 would SAFE (now HR 850), pick up again, this time with 258 co-sponsors.[264] In the Senate, McCain had a change of heart in 1999, and completely reversed his stance on encryption.[265] 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 security, and for other purposes" [emphasis added].[266] 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.[267]

---

[263] Diffie and Landau, *Privacy*, 223.
[264] "Security And Freedom through Encryption (SAFE) Act," 106th Cong., 1st sess., 1999, H.R. 695, http://thomas.loc.gov/cgi-bin/query/F?c106:3:./temp/~mdbsCYnyKP:e0: (accessed January 21, 2008)
[265] McCain may also have had his upcoming presidential bid in mind as a motivator for this change to the more politically popular position.
[266] "Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999," 106th Cong., 1st sess., 1999, S. 798, http://thomas.loc.gov/cgi-bin/query/D?c106:3:./temp/~mdbsD5PgHl:: (accessed January 21, 2008).
[267] Levy, *Crypto*, 305-6.

On September 16, 1998, Vice President Gore announced additional revisions to the Administration policy on encryption. First, it granted 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.[268]

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 180-degree turn 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 succeeded in overturning the export controls on encryption.

The Clinton administration's reversal of policy was a setback for the NSA. On the other hand, their rearguard action, throwing everything from alternative encryption standards (CCEP, DSS, Clipper Chip, etc.) to forcing modification of products during export reviews had produced some benefits, including the passage of CALEA, which will play a major role in the next chapter on Voice over IP. Perhaps more importantly, it had significantly delayed the spread of strong encryption for several years. For example, if one assumes that consumers replace their software products only every few years, then every copy of the 40-bit rather than 64-bit Lotus Notes represented a victory for the NSA. Given the NSA's history of technical innovation and its pre-existing advantage in cryptography, it undoubtedly bought itself some time—which may well have been all it sought to begin with.

---

[268] Albert Gore, News Briefing on Encryption (Sept. 16, 1998); Solveig Singleton, "Encryption Policy for the 21st Century: A Future Without Government-Prescribed Key Recovery," Policy Analysis Paper No. 325, Cato Institute, November 19, 1998, 16, http://www.cato.org/pubs/pas/pa325.pdf; 15 C.F.R. app. § 742.15(b)(3) (1999).

Chapter 3
Voice over Internet Protocol and the Federal Communications Commission

Introduction

This chapter explores how the FCC managed Voice Over Internet Protocol (VoIP) technology from the mid-1990s to present. The story of VoIP regulation at the FCC has a rather unique feature: forbearance. Contrary to what conventional wisdom about organizational behavior might suggest, the FCC executed a very deliberate strategy of *not* regulating VoIP during its early development so as not to hamper innovation. The FCC not only did not impose new regulation upon VoIP, it also actively refrained from imposing legacy regulations. What actions and reports the Commission did take sought to delay regulation. For example, the Commission avoided—and continues to avoid—formally defining or characterizing VoIP, which could potentially subject it to legacy regulation. Like the NSA in the previous chapter, the Commission sought to assert jurisdiction over its technology rather than allow other bureaucratic agencies to regulate it. However, the FCC did so in order to protect VoIP from regulation, rather than to impose additional regulation. The first regulation of VoIP in 2005 began only under intense pressure from federal law enforcement. The economic issues around VoIP, such as intercarrier compensation, remain largely unsettled.[269] This shows the FCC's continued reluctance to wade into this regulatory area before the technology is mature.

I argue that the FCC refrained from regulating VoIP because it recognized the uncertainties inherent in the emerging technology and sought to avoid hindering innovation through poorly written or poorly timed regulation. The Commission hoped that encouraging new technology to develop would promote competition in telecommunications, thereby improving consumer choice and welfare.[270] The deregulatory ideology of the era also played an underlying

---

[269] I use "access charges" and "intercarrier compensation" interchangeably. This is technically incorrect. Access charges are a subset of intercarrier compensation, along with reciprocal compensation. Although both are payments made between telcos, access charge rates are higher than intercarrier compensation rates.

[270] I also believe, although I cannot prove, that at least some people within the FCC hoped that VoIP would become a viable alternative to the PSTN and thereby force changes in the intercarrier compensation regime. The intercarrier compensation regime is widely believed to be irreparably tangled and a political minefield. The existence of large, wealthy, and political influential companies with entrenched interests in the current regime makes it nearly impossible to make any significant changes to the regime. Those who receive the access charge payments, which many analysts believe are far higher than the costs of providing the services for which payers are being charged, naturally wish to preserve the regime. Payers who may have to compete against new market entrants want to saddle their competition with the same costs, if they cannot get out of paying them themselves. (See later in chapter for more details.) Creation of an entirely new competitive technology could potentially undermine the entire regime, either making traditional telephony obsolete (as a critical mass of people switched to VoIP and abandoned their

role in the tendency toward not regulating. The Commission's foresight regarding the potential implications of regulation was most likely a result of the FCC's long history of dealing with emerging technologies. Prior experience had shown the problems that can arise when regulations and guidelines are poorly written, and the Commission chose forbearance as a solution because it believed that it is easier to regulate than to undo or change existing regulation.[271] Certainly, bureaucratic inertia, the resistance of entrenched interests, and the stifling of new challengers and interests could contribute to the difficulty of changing an existing regulatory regime. The existence of the FCC's internal think tank, the Office of Plans and Policy, most likely enhanced the Commission's willingness and ability to act with long-term consequences in mind.

Summary of Events

The most interesting feature of the history of VoIP regulation is the lack of action of by the FCC against a backdrop of rapid technological, economic and political changes. After the FCC was established in 1934, it faced a series of emerging and changing telecommunications technologies that taught it the value of restraint in regulation. For example, satellite communications, cellular technologies, and cable television all developed under the FCC's watch. During the 1950s and '60s, the development of minicomputers allowed for the merging of data processing and telephone communications, a new development in telecommunications. The FCC responded by initiating the *Computer Inquiries*, the first in a series of three inquiries designed to help the FCC better understand the emerging technology and its implications. *Computer I* marked the FCC's first attempt to create a framework for categorizing communications and data processing. Unfortunately, the framework was so ambiguous and confusing that it actually

---

wireline telephones) or uncompetitive. I believe that this was at least part of the unspoken motivation behind the FCC's willingness to grant VoIP developers so much leeway. Certainly all of the evidence – the forbearance, the attempts to protect the emerging VoIP providers against incumbents, the papers and speeches encouraging innovation on the Internet – all seem to fit this explanation. However, for perhaps obvious political reasons, no FCC officials will go on the record stating as much.

[271] The alternative explanation is that the FCC did not act because they did not know what regulations to impose, so they chose to do nothing. In this scenario, they could avoid being punished or ridiculed for imposing the 'wrong' regulation. In addition, the FCC's jurisdiction over VoIP was clear, so it was not ambiguity over who had authority over VoIP that caused the delay in action. I believe that forbearance is a relatively rare phenomenon in regulatory agencies. Discussion with a regulatory scholar at the Washington College of Law, American University, suggests that this is true. [Jeffrey S. Lubbers, personal communication, December 18, 2007.] Organizational theory suggests that organizations attempt to assert autonomy, expand bureaucratic turf, and protect their own interests, which suggests a tendency toward action rather than inaction. Theory suggests therefore that forbearance (which is deliberate, as opposed to inaction due to a desire to avoid punishment later) is unusual.

deterred potential entrants to the market, who could not figure out if they would be subject to regulation or not.

Soon thereafter, in 1969, the first ARPANET node was installed. The next decade saw the development of the personal computer, which would become critical to the future of VoIP, as well as the first packet voice experiments.

The rapid development of both computing and telecommunications technologies, and the general confusion over the framework set up by *Computer I,* prompted the FCC to launch *Computer II* in 1976. *Computer II* established the basic service versus enhanced services framework for regulating telecommunications: the former is highly regulated, the latter is not regulated. This bifurcation continues today, with the categories slightly modified by the Telecommunications Act of 1996. The landslide of regulatory obligations that categorization of VoIP could trigger is partly why the Commission sought to delay making such critical decisions about which, if any, regulations to impose on VoIP until 2004.

As *Computer II* wrapped up, the AT&T divestiture occurred. The breakup of AT&T opened the formerly monopoly telephony market to competition. The increased competition, coupled with rapid advances in computing technologies, led the FCC to initiate *Computer III,* which continues to present day.

Technologically speaking, very little VoIP development took place from the mid-1970s through the early 1990s. Not until the transition from NSFNET to the commercial Internet in 1995 did VoIP development pick up again, with the start of Jeff Pulver's Free World Dialup (FWD), an early bring-your-own-Internet-access Internet telephony service.

Meanwhile, two major pieces of legislation pertaining to telecommunications passed: CALEA, in 1994, and the Telecommunications Act of 1996. The 1996 Act was the first major update of telecommunications legislation since the 1934 Communications Act. It established the current categories of telephony, telecommunications (roughly equivalent to "basic services") and information services (roughly equivalent to "enhanced services") that still govern telecommunications today. The 1996 Act reaffirmed the FCC's jurisdiction over telecommunications and charged it with promoting competition in telecommunications. However, it also granted the Commission discretionary authority, including the discretion to forbear from regulating if the Commission found the sector to be sufficiently competitive.

Most of the FCC's actions pertaining to VoIP date from after 1996. Two important working papers on digital communications and the Internet were published in 1997 and 1999, arguing for restraint in regulation of the Internet and related technologies. The FCC also issued a report to Congress known as the Stevens Report in 1998, noting that the Commission had not determined an appropriate legal or regulatory framework for VoIP and would therefore refrain from regulating.

The first initiatives by incumbent telephone companies seeking to impose legacy telephony regulation on VoIP providers, or to capture the benefits of unregulated VoIP for themselves, also date from the late 1990s. The FCC confronted VoIP as a policy issue for the first time in March 1996, when the America's Carriers Telecommunication Association (ACTA) petitioned the FCC for a declaratory ruling that would, among other things, order VoIP providers to stop operating as unlicensed common carriers. A few years later, US West sought to have access charges imposed on phone-to-phone VoIP providers. The FCC did not act on the petition, and it was withdrawn. The issue came up again in 2002, when AT&T petitioned to have its phone-to-phone IP telephony service defined as an unregulated enhanced service. The FCC rejected the petition, declaring AT&T's service to be a telecommunications service like traditional telephony. A similar petition from Level 3 requesting forbearance in imposing access charges on VoIP was also submitted in 2003 and later withdrawn.

By late 2003 to 2004, three of the major players in the current VoIP market had entered: Skype, Vonage, and Comcast. Each of these three represented a different model of VoIP provider, although all three challenged the incumbent telcos. Both Skype and Vonage were bring-your-own-broadband VoIP providers, whereas Comcast also supplied the broadband connection. Of the three, only Skype did not interconnect with the public switched telephone network (PSTN). This lack of interconnection and physical facilities was critical, because these were the criteria the FCC would later use in choosing which VoIP providers to subject to regulation. In particular, in February 2004, the Commission ruled that IP-to-IP services such as pulver.com's Free World Dialup were unregulated information services.[272]

Around this time, FCC began coming under pressure from law enforcement to impose CALEA obligations on VoIP providers. In March 2004, the FBI, DEA, and DOJ together

[272] Federal Communications Commission, Memorandum Opinion and Order, Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, 19 FCC Rcd 3307, ¶ 9 (February 19, 2004) ("*Pulver Order*").

petitioned the FCC with a list of demands that would subject VoIP providers to the same CALEA requirements as traditional telephony. Arguably, the petition submitted by the law enforcement agencies (LEAs) actually required *more* access into VoIP communications than traditional telephony was subject to under CALEA. The FCC issued a Notice of Proposed Rulemaking (NPRM) in response. Over the next year, many different interest groups submitted formal comments: law enforcement agencies, incumbent telcos, VoIP providers, civil liberties groups, equipment manufacturers, and more. In August 2005, after considering the several rounds of comments, the Commission issued its first Report and Order (R&O) on CALEA, requiring some broadband and VoIP providers to accommodate wiretaps.

At around the same time, public safety concerns also forced the FCC to act on the question of E-911 (enhanced 911). VoIP-based 911 calls do not automatically give the caller's location, unlike traditional PSTN-based 911 calls. This disconnect caused delays that led to several highly publicized deaths. The resulting pressure forced the FCC to act. In August 2005, the FCC issued a Report & Order requiring VoIP providers that interconnect with the PSTN to make their systems compatible with the existing 911 location system.

In May 2006, the Commission issued its Second R&O on CALEA. This R&O affirmed the compliance deadline set in the first R&O, which was a victory for the LEAs. However, it also declined to intervene in developing CALEA compliance standards (technical standards), suggesting instead that industry and law enforcement should cooperate in finding mutually agreeable standards.

Overall, from the first packet voice experiments up through 2004, the FCC generally avoided regulating VoIP. Not until faced with pressure from law enforcement and public safety advocates did the Commission begin to impose regulations upon VoIP, preferring instead to let the technology develop free of regulatory restraint. The Commission hoped by not regulating, it could allow VoIP freedom to develop, and that time would resolve the technological, economic, and social uncertainties inherent in any emerging technology. This goal was particularly important because VoIP held the potential for technological innovation that could revitalize telecommunications, a critical sector of the economy. Thus, for more than a decade, the Commission exercised forbearance in regulating VoIP, allowing the technology to develop rather than prematurely impose potentially inappropriate regulations that could stifle innovation in a critical sector of the economy.

This page intentionally left blank.

VoIP Timeline

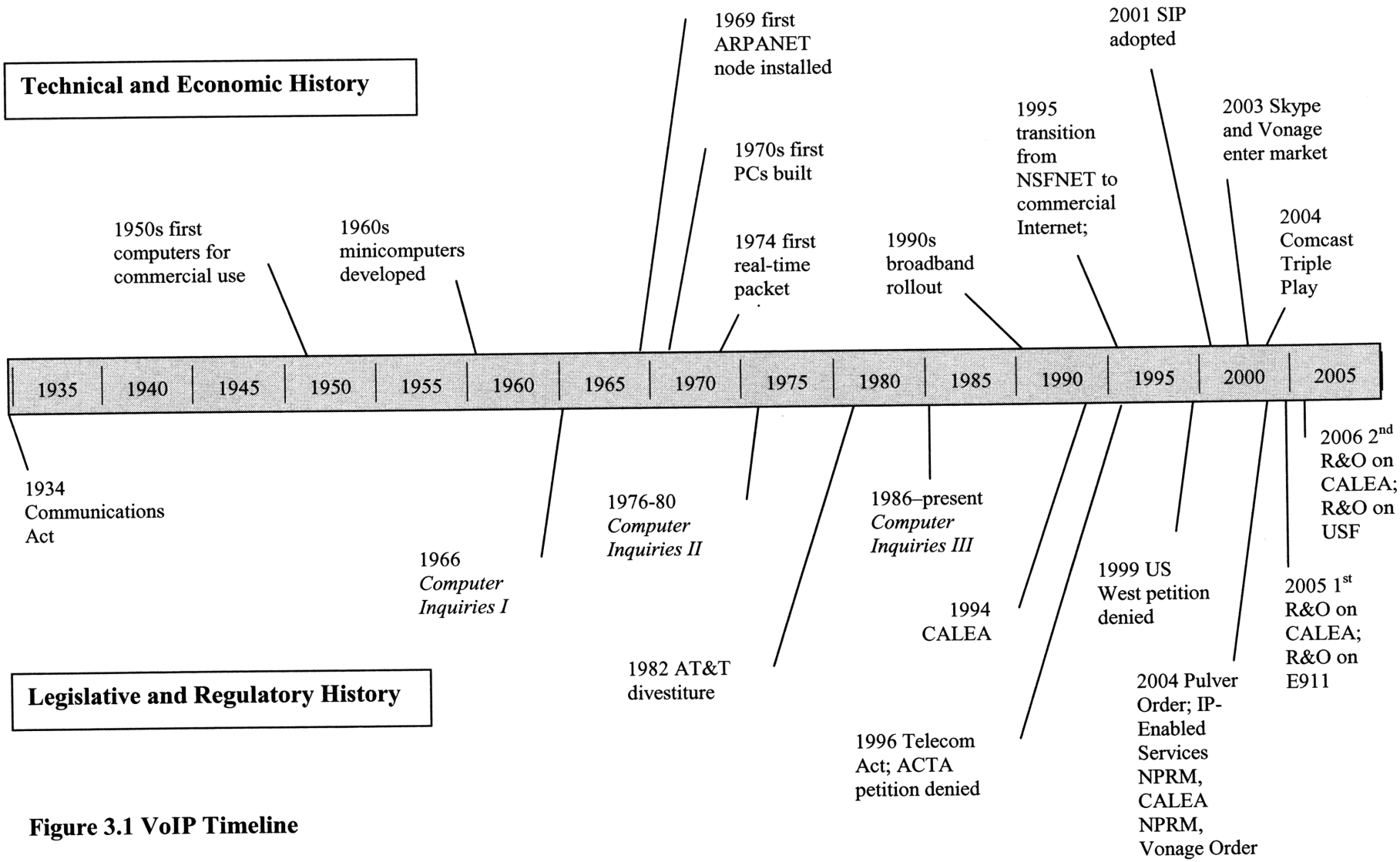


Figure 3.1 VoIP Timeline

This page intentionally left blank.

Roadmap of Chapter

The first three sections in this chapter provide background information needed to understand the regulatory challenges the FCC currently faces with respect to VoIP. The first section provides a brief definition and taxonomy of VoIP. It classifies varieties of VoIP according to the degree of interconnection with the public switched telephone network.

The second section describes technical developments, such as the Internet, the rise of personal computing, and the broadband rollout of the 1990s, that impacted and aided in the development of VoIP as we know it today. This section also walks through the evolution of VoIP technology from early incarnations such as Free World Dialup to current versions such as Skype, Vonage, and VoIP over cable.

The third section is a narrative of the legislative, judicial and regulatory history of telecommunications as it pertains to VoIP. The first half deals primarily with setting up the regulatory and legislative framework under which VoIP falls today. It begins with the Communications Act of 1934 and continues through the FCC's *Computer Inquiries,* which were interrupted by the AT&T divestiture, CALEA, and the Telecommunications Act of 1996. Many of the current regulatory issues and difficulties surrounding VoIP stem from a misfit between VoIP technology and the categories established by the legislation and regulation discussed in previous sections. This section also explains why seemingly simple question of 'what is VoIP?' is so important. Put simply, legislation and legacy regulatory frameworks divide telecommunications into one regulated and one unregulated sector. Therefore, deciding which category to put VoIP in is really a question of whether or not to regulate VoIP.

The second half of Section 3 covers actions more directly related to the FCC. It summarizes two working papers from the FCC's Office of Plans and Policy, the internal think tank, discussing the rationale behind deferring regulation of VoIP and other Internet technologies, a Report to Congress, and two critical *Orders*, the *Pulver Order* and *Vonage Order*. The two working papers help shed light on the motivations behind the Commission's actions. The *Pulver Order* is the first time the Commission formally categorizes any type of VoIP service, while the *Vonage Order* establishes FCC jurisdiction over VoIP.

The fourth section provides a breakdown of various regulatory issues around VoIP, dividing them into economic issues (disability access, universal service fund, and intercarrier compensation/ access charges) and security issues (CALEA obligations, E911). For the most part,

there has been little action on the economic issues, with the exception of the universal service fund. Most of the Commission's efforts have been directed at public safety (E-911) and security (CALEA). This final section shows how the Commission finally broke with its earlier pattern of avoiding regulation of VoIP under pressure from Congress (universal service fund and E911), and law enforcement (CALEA).

The following table summarizes the regulatory issues, challenges, and actions taken on VoIP issues.

Issue	Current Obligation	VoIP Challenges	Actions Taken
Disability Access	• Ensure that service and equipment are "accessible to and usable by individuals with disabilities, if readily achievable • Do not install equipment, features, or functions that do not meet these requirements • Provide relay services	• standardization of communications modes • funding	• None
Universal Service	• Contribute funds • Rreceive funds	• Should VoIP pay into or receive funds from the USF?	• Interconnected VoIP must pay into USF
Intercarrier compensation	• Access charges • Reciprocal compensation • Other forms of compensation (voluntary)	• Arbitrage opportunities created by IP • Separation of signaling and content • Who pays? How much?	• None
911/E911	• Identify emergency calls and route to PSAP • Provide callback information • Provide location	• Different identifier • Devices are nomadic (E911 services depended upon customer to provide location) • Separation of access, transport and application	• Interconnected VoIP must provide capability for geographic location identifier and connection to nearest PSAP
CALEA	• Provide call-identifying information • Provide content tracing (lawful intercept) capabilities • Ensure security and privacy	• Call-identification information unknown to service provider • Tension between wiretap, security, privacy and innovation • Who pays?	• Interconnected VoIP must provide CALEA intercept capabilities • Carriers assume responsibility for costs

Figure 3.2 VoIP Regulatory Issues[273]

[273] Many thanks to Chintan Vaishnav. Much of this chart and the content of the issue explanations are drawn from our chats and from his thesis. Chintan Vaishnav, "Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation" (Master's thesis, Massachusetts Institute of Technology, 2006), 88-93.

Section 1. Definition and Taxonomy

Voice over Internet Protocol (VoIP), or Internet telephony, can serve as either a replacement for traditional long-distance or international telephone service or as "an enhanced form of human-to-human communication based on the computer as the user interface rather than the telephone."[274] VoIP is voice communication transmitted in the form of packets over the Internet. In contrast, traditional telephony, also known as the public switched telephone network (PSTN), uses circuit-switching. Circuit switching opens a dedicated channel for each communication. No one else can use that channel for the duration of the call, even if no one is speaking at the time. In packet-switched networks, there is no dedicated channel. Instead, data is transmitted digitally in the form of packets and transmitted in bursts. Each packet has a header containing addressing information, and packets from the same message may arrive via different routes. The packets are then reassembled into the message at the destination.

By way of analogy, imagine a telephone call as a person (let's call him "Bob") trying to drive from Fenway to MIT. In a circuit switched network, it is as if police cordoned off a route from Fenway to MIT. The road is completely open, and only Bob's car is allowed on that route. If 'Charlie' is also trying to get from Fenway to MIT, he's out of luck: he has to find different road to drive on.

In a packet switched network, there is no exclusive use. Bob's car will take the fastest, least congested route to MIT. If Charlie is also trying to go to MIT, he may take the same route. Albert, who is going to Harvard, might share the road part of the way. If Bob has a long message, it may be divided among several cars (packets). Each car knows where it's going, and each car is numbered so the message can be reassembled in order once all the cars arrive. However, the cars may not take the same route. The first might take the Harvard Bridge. The second could take the same route, or it might take the BU Bridge. The third might loop around over the Longfellow Bridge. Nor do the cars necessarily arrive in the order they left. The third car might easily arrive before the second. However, once all the cars arrive, they are arranged by the end terminal (usually a computer) so that they are in the correct order.

VoIP may or may not include connections to the PSTN. It may connect on both ends, or only on one end. By some definitions, it may even connect to the PSTN on both ends. The

---

[274] David D. Clark, "A Taxonomy of Internet Telephony Applications," in *Internet Telephony,* eds. Lee W. McKnight, William Lehr, and David D. Clark (Cambridge, MA: MIT Press, 2001), 17.

degree of interconnection with the PSTN seems to be the key criteria the FCC has used in determining whether to apply telecommunications regulations to VoIP, so I adopt in this dissertation a taxonomy that classifies VoIP according to this variable. The FCC has not adopted a formal definition or classification for VoIP, but it has thusfar only applied regulation to interconnected VoIP, or VoIP technologies that interconnect with the PSTN on one end.[275] There are alternative classification systems for VoIP, such as a layers-based model, which arguably is a better fit with how VoIP technology actually operates.[276] However, since this dissertation focuses on regulation, I choose a classification system that better explains how regulation is imposed. An example of a VoIP classification system is the three-class version present by David Clark in *Internet Telephony* (1999).[277] Clark's three-class system is as follows:

- Class 1: Plain Old Telephone Service (POTS) over Internet, or PSTN-IP-PSTN
- Class 2: Hybrid POTS and Computer-based ITel, or PSTN-IP
- Class 3: Computer/ Internet-based ITel, or IP-IP

Class 1 uses Internet technology to provide long-distance or international POTS (plain old telephone service) telephony between existing telephones. Both end nodes are telephones, and the service looks exactly the same as circuit-switched POTS to the end user. Class 1 Internet telephony requires technology to convert signals between the PSTN and Internet networks. No conversion is required at the end nodes, because they are traditional telephones and not computers. An example of Class 1 Internet telephony is AT&T's current long-distance service,

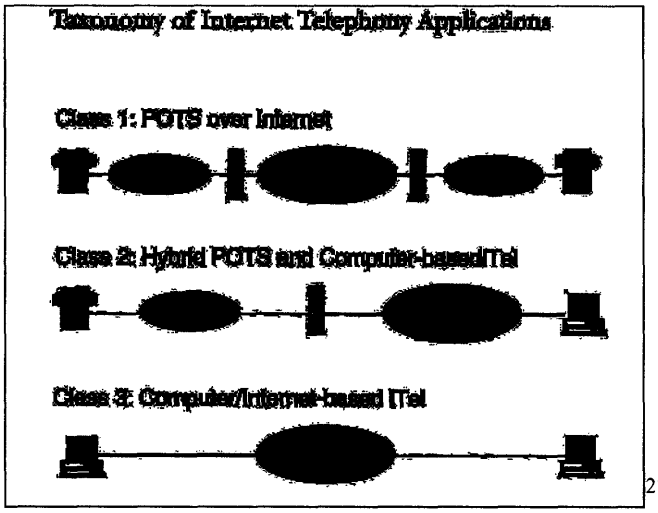
---

[275] Interconnection with the PSTN on both ends, the Class 1 VoIP discussed below, is treated by the FCC is functionally the same as traditional telephony.

[276] Nuechterlein and Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age* (Cambridge, MA: MIT Press, 2005), 209-213. From their footnotes (footnote 41 of Chapter 6), advocates of a layers-based model: Rob Frieden, "Adjusting the Horizontal and Vertical in Telecommunications Regulation: A Comparison of the Traditional and a New Layered Approach", 55 *Federal Communications Law Journal*, 207, 215 (2003); Craig McTaggert, "A Layered Approach to Internet Legal Analysis," 48 *McGill L.J.* 571 (2003); Philip J. Weiser, "Toward a Next generation regulatory Strategy," 35 *Loyola Univ. Chicago L.J.* 41 (2003); Kevin Werbach, "A Layered Model for Internet Policy," 1 *J. Telecomm. & High Tech. L.* 37, 38 (2002); Douglas C. Sicker & Joshua L. Mindel, "Refinements of a Layered Model for Telecommunications Policy," 1 *J. Telecomm. & High Tech. L.* 69, 71 (2002); John T. Nakahata, "Regulating Information Platforms: the Challenges of Rewriting Communications Regulation from the Bottom Up," 1 *J. Telecomm. & High Tech. L.* 95, 98 (2002). See also Richard S. Whitt, "A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model," 56 Indiana Journal of Law (2004), http://law.indiana.edu/fclj/pubs/v56/no3/Whitt%20Final%202.pdf (accessed January 26, 2008).

[277] Clark, "Taxonomy," 18-22.

which also terminates on the PSTN but routes the 'middle' of the connection over AT&T's Internet backbone.



[278]

Figure 3.3 Taxonomy of Internet Telephony Applications

Class 2 has one traditional telephone end node and one computer-based end node. It requires interoperability between the existing telephone network and Internet *and* between end nodes that are either existing telephone sets and/or computers. An example of Type 2 Internet telephony is a call from Vonage's telephone service to someone on the PSTN.

Class 3 is a purely Internet-based, packet-switched communication that does not interconnect with the PSTN or with traditional telephone end nodes. It is essentially a computer software application that runs over the Internet, with end node functionality residing in the computer. Skype and Free World Dialup are examples of Class 3 service.

A key difference between VoIP based telephony versus POTS is where the 'intelligence' in the network lies. Traditional telephony built a smart network with dumb end nodes. Most functionality resides in the network; the telephone handset is a very simple piece of equipment. In contrast, with VoIP, the computer end node is 'intelligent'. The computer packetizes the communication, addresses it, manages its delivery, reassembles received packets, etc. If the user desires, it can also choose the path the packet takes.

[278] *Ibid.* 19.

Packet switching allows for mixing voice communications with text, video, or other forms of communication, and delivered over the same copper pair (or other medium). The computer serves as call manager, keeping track of numbers, logging and archiving calls, assigning priority, and redirecting or forwarding as necessary. Traditional telephone features such as caller ID and call waiting are also handled by the computer rather than the network, which handles these functions in POTS. The computer can also control or alter user interface, providing greater variation than with traditional telephone handsets.

For the purposes of this thesis, I define VoIP as Class 2 and Class 3. I exclude Class 1 because the FCC has ruled that AT&T's phone-to-phone telephony a telecommunications service, which for regulatory purposes makes it the same as traditional telephony. [279] Class 3 services have been characterized as information services through the *Pulver Order*.[280] The characterization of Class 2 IP-to-PSTN services remains undecided.

---

[279] *Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, CC Docket No. 96-149, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 21905, 21957-58, ¶106 (1996) (*"Non-Accounting Safeguards Order"*).
AT&T asked the FCC to rule that because AT&T calls make use of Internet, it should be classified as an information service and exempt from access charges to LECs at each end of the call. At most, argued AT&T, it should owe only the lower business-line rate that ordinary ISP would pay for a connection to the LEC network under the "ESP exemption", which shields info service providers from an obligation to pay access charges to local telcos.

4/2004: FCC reaffirms tentative suggestion from 1998 that "phone-to-phone" VoIP offerings should be classified as telecommunications services subject to access charge obligations. (Report to Congress, *Federal-State Joint Board on Universal Service,* 13 FCC Rcd 11,501, ¶88 (1998), (*"Stevens Report"*, after Sen. Ted Stevens of Alaska, who sponsored the legislation requiring the report.) "FCC had defined a "phone-to-phone" VoIP provider as one that has the follow four characteristics: "(1) it holds itself out as providing voice telephony or facsimile transmission service; (2) it does not require the customer to use [customer premises equipment] different from that CPE necessary to place an ordinary touch-tone call (or facsimile transmission) over the public switched telephone network; (3) it allows the customer to call telephone numbers assigned in accordance with the North American Numbering Plan, and associated international agreements; and (4) it transmit customer information without net change in form or content." AT&T service met all four criteria. See Order, Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, 19 FCC Rcd 7457 (April 14, 2004), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-97A1.pdf (accessed August 11, 2007). ("AT&T Order").

From the summary of the ruling: "We clarify that, under the current rules, the service that AT&T describes is a telecommunications service upon which interstate access charges may be assessed. We emphasize that our decision is limited to the type of service described by AT&T in this proceeding, i.e., an interexchange service that: (1) uses ordinary customer premises equipment (CPE) with no enhanced functionality; (2) originates and terminates on the public switched telephone network (PSTN); and (3) undergoes no net protocol conversion and provides no enhanced functionality to end users due to the provider's use of IP technology."

[280] *Pulver Order*

Section 2. Technical History

This section discusses various technical developments in the history of VoIP, including enabling technologies that made VoIP possible and various forms of VoIP. The narrative is largely in chronological order, although most of the enabling technologies are by definition in the earlier part, and the actual VoIP technologies in the latter. Understanding the technical developments sets the background for the Section 3, which covers legislative and regulatory history. The relationship between technology and legislation and regulation – government action – is interactive. Although political science often takes technology as exogenous, technology is quite sensitive to legislation, judicial actions, and regulation. In some cases, government action can drive technological development through technology forcing (e.g., going to the moon, emissions standards for power plants). Perhaps more often, it can limit technology, determining whether it develops, when, in what form, and even how it is (or is not) deployed.

The emergence of new technologies can also affect competition. New technologies can compete with existing technologies or create new markets. The competition may not be limited to the economic sphere; competition may also exist over regulation. For example, regulation may favor existing actors, who will then seek to maintain the status quo, while challengers seek to change regulations. Just as likely is that the new technologies do not fit easily into the old regulatory frameworks. This is the case with VoIP. The mismatch between legislation and regulation written for the technologies of the POTS system and current VoIP technologies – in terms of VoIP not falling neatly into either of the categories of telecommunications established by legislation – is at the heart of much of the debate and controversy over VoIP regulation. Combined with a desire to promote innovation and competition, it helps explain why the Commission has refrained from regulating VoIP. In order to understand the disconnect between technology and regulation in VoIP, we first discuss the technology in this section, then the legislative/ regulatory history in sections 3 and 4.

The origins of what is now known as Voice over Internet Protocol (VoIP) date back to the early 1970s, soon after the installation of the first ARPANET nodes in 1969. ARPANET was

the world's first functional packet-switched network, the grandfather of today's Internet.[281] ARPANET was a project of the Advanced Research Projects Agency (ARPA, now DARPA, Defense Advanced Research Projects Agency) of the Department of Defense (DOD). Packet-switching, which now powers most communications networks, was a new and untested concept until ARPANET. Before ARPANET, communications were circuit-switched, which required a dedicated line that was occupied for the entire length of the call between two parties. Packet-switching allowed for sharing of the line and separate routing of each packet, which greatly increased the functional capacity of a network.

The establishment of the ARPANET, which ran over leased lines, allowed for the first demonstration of real-time packet voice between USC's Information Sciences Institute and MIT's Lincoln Lab in 1974. The first papers exploring the possibility of packet-switched voice had been published just a few years earlier. A more formalized exploration began with the publication of the first Request for Comments (RFC 741) for packet voice in 1977.[282]

After these experiments, packet voice entered what amounted to a 15-year lull until the 1990s. The proliferation of packet switched networks during this period, most of them for research purposes allowed for further experiments in the 1990s on DARTnet (Defense Advanced Research Testbed Net) and the Mbone, which carried the first multicast Internet Engineering Task Force (IETF) meetings. During this period, most Internet telephone calls took place between research labs, targeted primarily at multi-party teleconferences rather than person-to-person calls.[283] Internet telephony did not exist in its present form, as a viable alternative to traditional telephony. Connections to the NSFNet were still largely limited to universities and research facilities, and broadband capabilities were rare.[284] There simply was not enough bandwidth to make calls of tolerable quality, and running voice applications over narrowband,

---

[281] For an excellent history of the creation of ARPANET and the Internet, see Janet Abbate, *Inventing the Internet* (Cambridge: MIT Press, 1999). See also the Internet Society Society, "Internet History," http://www.isoc.org/internet/history/brief.shtml (accessed August 11, 2007).

[282] RFCs are a series of memoranda on Internet protocols, standards, innovations, and research. The process originated with the ARPANET, when Steve Crocker of UCLA, home to one of the first Interface Message Processors (IMPs, similar to today's Internet routers), typed a paper memorandum on host software and tacked it to a hallway bulletin board for other ARPANET researchers. He titled it "Request for Comments", and the title has stuck. This document became the first in the series. The RFCs are now a formalized series of memoranda that together form a history of the evolution of Internet standards and other innovations. The series is officially managed by the Internet Engineering Task Force, although actual management has been contracted out to USC's Information Sciences Institute.

[283] Henning Schulzrinne, "Internet telephony," *IEEE Network* 13 (May/June 1999): 6-7, http://ieeexplore.ieee.org/iel5/65/16630/00767131.pdf?arnumber=767131 (accessed August 11, 2007).

[284] *Ibid.*

dial-up Internet connections produced "some of the most garbled, inaudible conversations since tin can met string."[285]

Soon after the transition from the NSFnet backbone to what we know as the commercial Internet on April 30, 1995, the first viable commercial and non-commercial VoIP services appeared. (Note that the Internet transition did not occur until a year after CALEA, which was written for telephony, passed.) VocalTec introduced Internet Phone, one of the first commercial PC-based Internet telephony software programs.[286] VocalTec also introduced a piece of software called VocalChat, which used a LAN of connected computers as an intercom system. Users had to provide their own Internet connection.[287] That same year, Jeff Pulver launched Free World Dialup, a non-commercial VoIP network from pulver.com. FWD served as a directory service that allowed users to make free telephone calls to other FWD users around the world. FWD provided no transmission functionality; like the VocalTec and other offerings of the time, it was "bring your own broadband".[288] Free World Dialup would later be the subject of a FCC decision, the *Pulver Order,* that has helped shape how the FCC characterizes VoIP.

Around this time, the 'traditional' telephone companies, such as AT&T, began transitioning many of their long-distance services to the IP backbone. That is, they continued to provide long distance service, but as a Class 1 VoIP service. The calls still originated and terminated on the PSTN, but ran over the IP backbone in the middle. Each of these different type of IP-based telephony offerings, from the Class 3 of Free World Dialup to Class 1 of AT&T, would soon be the subject of various petitions to the FCC in coming years.

Throughout this period, debates over protocols for VoIP continued. Several protocols are still in use, although the best known is the multi-purpose Session Initiation Protocol (SIP), which was adopted by the IETF as a standard in 2001. SIP is an application layer control protocol (signaling protocol) for initiating, modifying, and terminating sessions. It is used most commonly for setting up and taking down voice and video-based calls. Perhaps more importantly, it was designed to support the building of many of the call processing functions available through the PSTN, such as dialing numbers, dialtones, ringtones, and busy signals, as well as

---

[285] Jeff Bertolucci, "Internet Phones: Clear Winners," *PC World,* May 1, 2004, (http://www.pcworld.com/reviews/article/0,aid,115053,00.asp), cited in Nuechterlein and Weiser, *Digital Crossroads*, 192.
[286] See review of VocalTec Internet Phone at http://blog.tmcnet.com/blog/tom-keating/voip/voip-history.asp
[287] http://www4.dogus.edu.tr/bim/bil_kay/network/intranets/ch32.htm (accessed August 3, 2007).
[288] Nuechterlein and Weiser, *Digital Crossroads*, 198.

other functions provided by Signaling System 7 (SS7), the protocol used on the PSTN.[289] That is, it was almost explicitly designed so that it could allow VoIP to function as a substitute for traditional telephony.

The significance of SIP is that it takes away some of the advantage that telecom players who control the physical network have.[290] Traditionally, because the intelligence in telephone networks is in the network, rather than in the 'dumb' terminals (telephones), whoever controlled the physical layer could also control applications. With the Internet, the intelligence is in the end nodes (computers), and the network is 'dumb'. Voice calls, like all applications, are just packets – and more importantly, no longer under the control of proprietary telephone software in centralized circuit-switches. Thus VoIP is a medium for innovation just as any application that runs over the Internet is a medium for innovation.[291] SIP is particularly significant in this respect because it is an open protocol, developed by the Internet community rather than its rival H.323, which was largely developed by telecom players.

On the consumer side, VoIP was not well-known among consumers during this period, and even farther from becoming a viable alternative to traditional telephony. Technical, economic, and social obstacles to its widespread deployment remained unsolved.[292] Many of these would later be resolved with the widespread deployment of broadband. However, in the late 1990s and early 2000, broadband subscriptions in the U.S. were still relatively low, even

---

[289] From various discussions with Chintan Vaishnav and David Clark, I gather that SIP is something of a 'garbage can' protocol: not particularly lean, but contains something for almost everyone. Not all VoIP communications use SIP. For example, the International Telecommunications Union (ITU) endorses H.323, which was largely written by telecom corporations, whereas SIP is considered more of a product of the IP/ Internet community. Skype uses a completely separate and proprietary protocol.

For a summary and explanation of the difference between the various VoIP protocols that goes into much greater technical depth, please see Vaishnav, "VoIP." See also http://www.processor.com/editorial/article.asp?article=articles/P2738/24p38/24p38.asp&guid=. For an explanation of SIP, see Henning Shulzrinne's, "SIP: Session Initiation Protocol," at http://www.cs.columbia.edu/sip/ (accessed February 1, 2008). Schulzrinne and Mark Handley wrote SIP. For history of SIP, See Internet Engineering Task Force (IETF), "Sessions Initiation Protocol (sip) Charter," http://www.ietf.org/html.charters/sip-charter.html (accessed February 1, 2008); Session Initiation Protocol (SIP) Working Group, "SIP WG Supplemental Homepage," http://www.softarmor.com/sipwg/ (accessed February 1, 2008); Wikipedia, "Session Initiation Protocol," http://en.wikipedia.org/wiki/Session_Initiation_Protocol (accessed February 1, 2008).

[290] As the Net neutrality debates show, however, it does not quite take away all of the advantages of control over the physical layer. Packet discrimination is one of the most controversial issues in the Net neutrality debate. Packet discriminiation is the practice of distinguishing between packets carrying different types of data (or from different sources), and treating them differently. For example, there have been several cases in which local telephone companies have deliberately blocked or degraded service for VoIP users in order to hinder their competitors. See Jonathan Krim, "FCC Probes Blocking of Internet Phone Calls," *Washington Post,* February 17, 2005, E01.

[291] Nuechterlein and Weiser, *Digital Crossroads*, 192.

[292] The following list of obstacles – quality of service, pricing for enhanced service, reliability, always-on connectivity, and ubiquitous deployment – is drawn from David Clark, "Taxonomy," 23-24.

though cable and telephone providers had spent much of the previous years laying massive quantities of optic fiber to the home during the telecom boom.[293] Most households with Internet access were still using dialup, which is not connected all the time.

Since using Internet telephony as a viable alternative to traditional telephony requires an always-on connection to a packet-switched network, dialup connections, unless given a dedicated line, would not work. People are accustomed to having telephone service 24/7, with calls always 'going through'. This imposes an additional requirement: improving the reliability of the inherently unreliable IP, which was designed as a 'best effort' protocol, to the very low error or failure rates of the PSTN.

Another aspect was quality of service (QoS). The higher speeds (more bits per second) of broadband considerably reduced this problem. However, VoIP call quality is still inferior to that of circuit-switched telephony, which dedicates a full 64 kbps circuit to each call. Achieving similar call quality with VoIP, even with broadband connections, may require the ability to ensure prioritization of a stream of packets to ensure that this lag- and jitter-sensitive data stream would not suffer from intolerable (to the human ear) deterioration of service.

On the economic front, the QoS requirements in turn might necessitate pricing mechanisms to limit use (if every packet is prioritized, then none are) and compensate the provider. Lastly, Internet telephony, like traditional telephony, is subject to network effects. The networks' appeal and value increases exponentially (up to a point) with the number of users: a network that connects to only a few users has little total value, whereas one that connects to many has a much greater value. With few users (and little to no ability to connect to the PSTN), the early VoIP technologies simply were not appealing to a nation where everyone had a telephone.

VoIP did not become a viable alternative to traditional telephony in the residential market until 2002-2004.[294] (Class 1 VoIP, such as AT&T's "phone-to-phone" VoIP, began a little

---

[293] Ken Belson, "Telephone Line Alchemy: Copper Into Fiber," *New York Times,* October 11, 2004, http://www.nytimes.com/2004/10/11/technology/11fiber.html?ex=1255147200&en=35c96d27d44f239a&ei=5088&partner=rssnyt (accessed December 3, 2007).
For broadband deployment figures, see Organization for Economic Cooperation and Development, "OECD Broadband Portal," http://www.oecd.org/sti/ict/broadband (accessed December 3, 2007). Under graph titled "Households with Broadband Access (2000-2006)", OECD lists 4.4% of US households as having access to broadband in 2000. The figure had jumped to 22.1% by June 2007, for a total of 66.2 million subscribers. See graph "OECD Broadband subscribers per 100 inhabitants, by technology, June 2007" and "Total Broadband Subscribers by Country (June 2006)."

[294] VoIP services for corporate use were adopted far earlier.

earlier, around the turn of the century.) By this time, enough homes had broadband connections – often through cable broadband rather than DSL through traditional telcos -- to make VoIP a viable option. The first VoIP companies into the commercial market were bring-your-own-broadband providers, such as Skype and Vonage.

Vonage launched its VoIP service in March 2002.[295] Until early 2007 it was the leading VoIP provider, serving up to 2.5 million subscribers.[296] Under the classification schema laid out in the taxonomy section, Vonage is a Class 2, or IP-to-PSTN VoIP service. A Vonage subscriber uses an ordinary telephone number and can both reach and be reached by anyone on an ordinary telephone network, anywhere in the world. This allowed Vonage to take advantage of the network effects of the existing POTS from the start. Vonage and other forms of Class 2 VoIP therefore formed the first viable substitute for traditional circuit-switched telephony.[297]

Vonage began offering its service for $5 per month. (Current rates are around $25-30 a month.) The subscriber had to provide his own broadband connection, but beyond that, all calls, both local and long distance, are included in the monthly fee. Vonage, like most of its competitors, offered unlimited calling.

A Vonage subscriber places a call by connecting a regular telephone into a Vonage-provided adapter associated with an IP address. The adapter is then connected to a broadband connection provided by the customer, e.g., DSL or cable broadband service. If the person being called is also a Vonage subscriber, then the service functions as a Class 3 VoIP service – a directory service that connects and terminates on the Internet. However, if the Vonage subscriber is calling someone on the PSTN, then Vonage will convert the call from IP to SS7 (the standard format used by circuit-switched networks) and drop the call off on the network of a partnered telecommunications wholesaler who finishes delivering the call.

To a PSTN subscriber calling a Vonage subscriber, the Vonage subscriber is indistinguishable from an ordinary telephone subscriber. Vonage, through its wholesale partners, obtains telephone numbers managed by the North American Numbering Plan Administration (NANPA) and assigns them to its subscribers. However, the Vonage subscriber's phone number is functionally more like an e-mail address: it is geographically portable. The phone number is

---

[295] The name "Vonage" is a play on words: VON Age, or Voice-Over-the-Net Age. "VON" is another name for VoIP, which is also called Voice over Broadband, Internet telephony, or IP telephony.
[296] Vonage, "About Us: Timeline," http://www.vonage.com/corporate/about_timeline.php (accessed December 3, 2007).
[297] Vonage, "Timeline"; Nuechterlein and Weiser, *Digital Crossroads*, 201-4.

simply a proxy for the IP address associated with the Vonage adapter. Therefore, the subscriber can take his adapter with him anywhere in the world, and receive calls as if he is at home, in his home area code. For example, the subscriber can have a 617 Boston area code, but if he takes his adapter with him to Los Angeles, his friends in Boston can call him and still only be charged for a local call. The IP packets will follow him to his adapter wherever in the world he is. In addition, more than one telephone number, in more than one area code, can be associated with the adapter. Thus he could have both a Boston (617) number and a Los Angeles (213) number, so his LA-based friends could make 'local' calls to him when he is in Boston as well.

The flexibility of Vonage (and similar) services raises two regulatory issues. First, there is a limited number of telephone numbers, so assigning multiple numbers to each VoIP subscriber could significantly speed up the depletion of telephone numbers. This issue will not be discussed in this dissertation.[298] The second issue is access charges (intercarrier compensation), which will be discussed in a later section. By allowing VoIP users to access the PSTN without placing conventional long distance calls (with attendant access charges), LECs potentially lose billions of dollars in implicit cross-subsidies.

A different type of VoIP, Skype, launched a year later in August 2003.[299] Skype began as a Class 3, IP-to-IP VoIP service. The service is free. The customer provides their own computer, a headset or microphone (input-output device), and their own broadband connection. To use Skype, the customer simply downloads the Skype software. Skype provides a directory of Skype users, informing members when other members are present and at what IP address. (Actually the IP address is not explicitly revealed, although clicking on an available member will directly connect the user.) The actual call, which can include video, text, and file transmissions, is performed on a peer-to-peer (P2P) basis. Skype does not provide transmission functionality. Unlike Vonage, Skype users can only call one another, much as AOL's Instant Messenger (IM) customers can only contact each other. Both parties to the call must have their own broadband

---

[298] NANPA has already had to increase the number of area codes in order to expand the available pool of telephone numbers due to the popularity of fax lines and cell phones. Assigning multiple numbers to each device, such as a Vonage adapter or SIP phone, could potentially drain the dwindling pool of numbers much faster. The problem is that the other way to expand the available pool of numbers, such as adding an extra digit, would require massive telephone infrastructure upgrades. Ben Charny, "FCC to vote on phone-number crunch," CNET News.com, March 28, 2002, http://www.news.com/FCC-to-vote-on-phone-number-crunch/2100-1033_3-870832.html, (accessed January 7, 2008); Ben Charny, "Are 12-digit phone numbers in our future?" ZDNet News, March 28, 2002, http://news.zdnet.com/2100-1009_22-870880.html (accessed January 7, 2008).

[299] Skype, "About Skype," http://about.skype.com/ (accessed December 3, 2007). Search in the News Archives to compile a timeline. See also Wikipedia, "Skype," http://en.wikipedia.org/wiki/Skype (accessed December 3, 2007).

connections. Basic Skype users cannot call customers on the PSTN. Nor do they receive telephone numbers so that PSTN users can call them.[300] Both Skype and Vonage-type services would later be the subject of FCC orders addressing VoIP "characterization" issues: respectively, the *Pulver Order* and the *Vonage Order.* (See Section 3)

Soon after the introduction of Skype and Vonage, the broadband providers saw the challenge (or opportunity) in VoIP. For Comcast, it was an opportunity to put the fiber it had already run into millions of homes to another use for very little additional cost. Comcast introduced the "triple play"--bundled cable, digital TV, and unlimited local and long distance calling--in June 2004 for $90 a month. Given that many consumers already paid $90 for the cable and digital TV alone, Comcast was functionally giving away telephone service. The consumer response was very favorable.[301] Verizon, seeing its core business being snatched away by upstarts like Vonage, and more worrisome, other 800-pound gorillas like Comcast, began offering its own VoIP products as well in 2004. Verizon, like other landline telcos, was already bleeding from the growing number of customers who were abandoning landline telephones altogether in favor of their cell phones. Although offering VoIP undercut its own traditional landline business, losing customers to Comcast altogether was even worse, so Verizon's VoIP offerings included both bundled and bring-your-own-broadband service (VoiceWing).[302]

As predicted by Nuechterlein and Weiser in 2005, in the past few years the trend has been away from bring-your-own-broadband and toward more familiar providers such as the cable companies and telephone companies.[303] Vonage's legal troubles over patents, falling share

---

[300] Its SkypeOut service, which allowed Skype users to call numbers on the PSTN, began a year later in July 2004. This gave Skype IP-to-PSTN capability, but not PSTN-to-IP capability. In April 2005, Skype introduced SkypeIn, which gave Skype users the option to buy a telephone number so that PSTN users could call them. With both SkypeOut and SkypeIn activated (both are fee services), Skype is functionally a Class 2 VoIP service. However, for purposes of this dissertation, when I refer to Skype, I am referring to the original IP-to-IP, Class 3 VoIP service without interconnection to the PSTN. Pulver's Free World Dialup is another example of a Class 3 service, but I use Skype as an example because it is better known. The fact that its headquarters are in Luxembourg also helps illustrate some of the jurisdictional issues facing regulators.

[301] Ken Brown, "Cablevision to Offer Internet Phone-Call Bundle," *Wall Street Journal,* June 21, 2004, B5; Ken Brown and Almar Latour, "Phone Industry Face Upheaval as Ways of Calling Change Fast," *WSJ,* August 25, 2004, A1, cited in Nuechterlein and Weiser, *Digital Crossroads*, 196.

[302] Greg Galitzine, "Verizon VoIP Service Takes Wing," Greg Galitzine's VoIP Authority Blog, entry posted July 22, 2004, http://blog.tmcnet.com/blog/greg-galitzine/voip/verizon-voip-service-takes-wing.html (accessed December 3, 2007).

[303] Nuechterlein and Weiser, *Digital Crossroads*, 196-7.

prices, and market share,[304] and the demise of the number-two bring-your-own-broadband VoIP provider SunRocket in July 2007, are indicators of this trend.[305] As Nuechterlein and Weiser noted, the lower costs of VoIP relative to conventional circuit-switched telephony would induce consumers to switch, particularly as more and more other consumers made the switch, and they would be inclined to purchase VoIP from established providers rather than unknown upstarts.[306] They further reason that for simplicity's sake, most consumers would rather deal with one service provider rather than two, and would therefore be more inclined to purchase VoIP services from their broadband provider.[307] (Comcast, in particular, has ad campaigns emphasizing precisely this "one bill" convenience.) The Yankee Group's most recent study in 2007 notes that this trend continues: Comcast exceeded the number of Vonage VoIP subscribers for the first time in the first quarter of 2007.[308]

It took about thirty years from the first packet voice experiments for VoIP to emerge as a full-fledged commercial technology and a viable challenger to the existing telephone industry. Unfortunately, during that thirty year period, legislation did not quite evolve to accommodate it.

---

[304] Steven Musil, "Week in Review," CNET News.com, August 10, 2007, http://news.com.com/Week+in+review+Patent+woes/2100-1083_3-6201874.html?tag=item (accessed December 3, 2007).

305 Matt Richtel, "Internet Phone Company Halts Operations," *NYT*, July 17, 2007, at C2. http://www.nytimes.com/2007/07/17/business/17sunrocket.html?ex=1342324800&en=7dd5746aad3172e0&ei=5090&partner=rssuserland&emc=rss

[306] Daniel Klein, "Why Vonage Is Just a Fad," ZDNet.com, May 19, 2004, http://techupdate.zdnet.com/techupdate/stories/main/Why_Vonage_Just_Fad.html?tag=tu.arch.link (accessed December 3, 2007); Dinesh C. Sharma, "Study: Cable Giants to Flex VoIP Muscle," CNET News.com, August 3, 2004, http://news.com.com/Study%3A+Cable+giants+to+flex+VoIP+muscle/2100-7352-5295023.html?part=dtx&tag=ntop (accessed December 3, 2007), describing Yankee Group study predicting that established broadband providers will soon overcome the early lead of the unaffiliated VoIP providers like Vonage; Dinesh C. Sharma, "VoIP Picks Up Momentum," CNET News.com, August 30, 2004, http://news.com.com/VoIP+picks+up+momentum/2100-7352_3-5330123.html?tag=item (accessed December 3, 2007), predicting that cable providers will gain a 56% market share at the end of 2004, with alternative voice providers continuing to fall from their 66% 2003 market share to a 19% market share in 2005.

[307] Nuechterlein and Weiser, *Digital Crossroads*, 196.

[308] Paula Bernier, "Yankee Group: Comcast Exceeds Vonage in VoIP Sales," *New Telephony,* August 1, 2007, :http://www.newtelephony.com/news/78h116948.html (accessed August 18, 2007). "According to the report, in the first quarter of 2007 Comcast for the first time exceeded Vonage's subscriber base, with 2.4 million subscribers. This is indicative of a larger trend, notes Yankee, which reports that in 2006, the consumer VoIP market grew 127 percent to 9.1 million subscribers, increasing from 4 million subs in 2005. The firm says that MSOs drove most of that growth, adding 3.9 million subs to reach 6.3 million subs at the end of 2006. For 2006, cable companies owned 69 percent of the VoIP marketshare whereas "bring-your-own-broadband" VoIP providers like Vonage claimed 31 percent of the market. FTTP-based VoIP – from fiber-fueled telcos like AT&T and Verizon, which offer VoIP as part of a bundle of services – accounted for less than 1 percent share, Yankee says. (This report doesn't take into consideration PC-based VoIP applications from such companies as Yahoo! and Skype, which are in use by 15 percent of U.S. households.)"

Instead, as we will see in the next section, legislation was written with the old telephone architecture in mind -- a framework that neither the Internet nor VoIP quite fits.

Section 3. History

This section discusses the legislative and regulatory history of VoIP beginning with the establishment of the FCC in 1934 through 2004. The Commission's more recent regulatory actions, as opposed to the inaction of this period, are covered in Section 4. The history sets up the legislative and regulatory framework that governs VoIP today, namely the 1996 Telecommunications Act. In particular, this section discusses the division of communications into two categories, telecommunications service and information services, that was set up by the *Computer Inquiries II* and the Telecommunications Act of 1996. The codification of these two categories has profound influence on the current regulatory status of VoIP, because these categories were established for the technology of the traditional telephone system. They did not take into account the very different architecture of the Internet, which is the basis of VoIP. Thus, VoIP does not fit neatly into either category, but instead has characteristics of both. Unfortunately, since telecommunications services are highly regulated and information services unregulated, characterizing VoIP as one or the other has enormous regulatory significance. The discussion of the 1996 Act also explains the legal justification for the FCC's forbearance.

The breakup of the Bell system is also covered briefly covered. The end of the Bell monopoly on telephone service set the stage for the entry of many new actors in the telecommunications industry. It also drove the creation of the extremely convoluted access charge regime that is the subject of much litigation.

There is a brief sidebar into the Broadband Inquiries. This digression exists simply to show that the FCC had a history of dealing with emerging technologies by attempting at an early date to anticipate technical developments and their potential implications.

The final part of this section explores two key white papers issued by the FCC's Office of Plans and Policy, their internal think tank. The two papers set up the justification for delaying regulation of the Internet and VoIP in the interests of promoting technological innovation.

Communications Act of 1934

The Communications Act of 1934 created the Federal Communications Commission (FCC) and united authority over telecommunications under a single agency. The 1934 Act granted the FCC jurisdiction over "all interstate and foreign communication by wire and radio, telegraphy, telephone and broadcast".[309] Previously, the Federal Radio Commission (FRC), Interstate Commerce Commission (ICC), Post Office Department, and Department of State all shared authority over one or more technologies, which greatly complicated regulation. In addition, some government officials felt the ICC neglected telephone carriers because it was preoccupied with regulation of railroads.[310]

The Act charges the FCC with regulation of non-federal government use of the radio spectrum (such as radio, television broadcasting and cellular phone spectrum), all interstate telecommunications, and all international communications that originate or terminate in the U.S.. It is divided into seven bureaus. The Wireline Competition Bureau (WCB) handles most VoIP issues. Additionally, the FCC consists of several offices that provide support services to the Bureaus. For this thesis, the most relevant one is the Office of Strategic Planning & Policy Analysis (OSP), formerly the Office of Plans and Policy (OPP). The OSP is the FCC's internal think tank, charged with identifying policy objectives for the agency and monitoring the communications industry to identify trends, issues and overall industry health. The OSP works closely with the FCC Chairman, acting as consultants to the Commission in areas of economic, business, and market analysis. "The Office also reviews legal trends and developments not necessarily related to current FCC proceedings, such as intellectual property law, the Internet, and electronic commerce."[311] Two key white papers from the OPP that lay out the justification behind refraining from regulation of VoIP and other Internet technologies will be discussed in a later part of this section.

The bill was not meant to be particularly controversial or effect major changes. The Congressional Record states that "[t]he bill as a whole does not change existing law, not only with reference to radio but with reference to telegraph, telephone, and cable, except in the

---

[309] FCC, "History of Wire and Broadcast Communication," http://www.fcc.gov/cgb/evol.htm, May 1993, quoted in Cybertelecom, "Communications Act of 1934," http://www.cybertelecom.org/notes/communications_act.htm (accessed August 3, 2007).

[310] Henk Brands and Evan Leo, *The Law and Regulation of Telecommunications Carriers* (Artech House Publishers 1999), 4, in Cybertelecom, "Communications Act of 1934."

[311] Wikipedia, "FCC," http://en.wikipedia.org/wiki/Fcc (accessed August 3, 2007).

transfer of jurisdiction [from the ICC to the FCC] and such minor amendments as to make that transfer effective."[312] However, one clause would come to have great significance in the decades to come: the provision granting the FCC jurisdiction over *interstate* communication. At the time, only two percent of telephone traffic was interstate, while the other 98 percent was intrastate.[313] However, technologies and usage patterns have shifted significantly since then, such that interstate calls now make up a much greater proportion of calls.[314] One of the first steps the Commission has taken with regards to Internet and VoIP regulation, therefore, has been to assert the interstate nature of both. More accurately, in the case of VoIP, it has asserted that the interstate and intrastate components of VoIP are inherently inseparable, which puts VoIP under FCC jurisdiction.[315] As discussed later (see *Vonage Order*), this has enabled the FCC to shield VoIP from impending state regulation and delay imposition of federal regulation.

The text of the bill also establishes the concept of a telephone carrier as a "common carrier."[316] The concept of common carriage is important for VoIP because "telecommunications service", which will come up in later sections as one of the two regulatory categories VoIP could fall into, is essentially synonymous with "common carriage".[317] The concept of common carriage derives from English common law. The usual test for a common carrier is whether it is a "provider of transmission services that (i) holds itself out to serve all customers interested in buying any services the carrier offers and (ii) allows customers to transmit whatever content they wish by means of its facilities. Stated simply, common carriers—as opposed to "private carriers"—do "not make individualized decisions, in particular cases, whether and on what terms to deal."[318,319]

---

[312] Communications Act of 1934, 47 U.S.C., 78 Cong. Rec. 10,313 (1934), http://www.fcc.gov/Reports/1934new.pdf

[313] Milton Mueller, "'Universal service' and the new Telecommunications Act: Mythology Made Law," *Communications of the ACM,* March 1997, http://www.vii.org/papers/cacm.htm, quoted in Cybertelecom, "Communications Act of 1934."

[314] The FCC has helped assure this shift by declaring most Internet usage to be interstate. See *Pulver Order* and Memorandum Opinion and Order, Vonage Holding Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission, 19 FCC Rcd 22404 (November 9, 2004), ("*Vonage Order.*")

[315] *Vonage Order*

[316] The bill's own definition of "common carrier" is rather circular: "The term "common carrier" or "carrier" means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this Act; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier." 47 U.S.C. 153(10).

[317] Nuechterlein and Weiser, *Digital Crossroads*, 76

[318] An alternative definition: "Common carriage was applied to freight or carriage companies and inland and ocean water carriers. By common law, common carriers were 1) required to serve upon reasonable demand, any and all

Explanations for the rationale behind regulating common carriers varies, although most seem to cite some combination of the prevention of exploitation of market or monopoly power, prevention of discrimination, and the importance of network transport and infrastructure to national security and economic growth.[320] The belief in the importance of common carriage is the basis for subjecting "telecommunications carriers," which are a subset of common carriers, to regulation.[321] This concept will be discussed more in the section on the Telecommunications Act of 1996.

Computer Inquiries - Background

The FCC has a long history of dealing with the nexus of the computer services industry and communications industry, beginning with the Computer Inquiries in 1966. The initial Inquiry evolved into a series of three Inquiries that continues to shape the telecommunications to this day. However, a little background is necessary to understand how the computers and communications industries came to intersect.

The first computers designed for commercial use appeared on the market in the mid-1950s. Most of these automated routine information processing – payrolls and checks, bills in telephone and utility companies, records and sorting of bank checks, orders, inventory management. These were soon followed by applications combining data processing and communications, such as American Airlines' automated reservation service, SABRE. Generally these computer data processing systems were developed to help support companies' primary business, which usually was not communications or data processing.[322]

---

who sought out their services; 2) held to a high standard of care for the property entrusted to them; and 3) limited to incidental damages for breach of duty." Quote from Eli M. Noam, "Beyond Liberalization II: The Impending Doom of Common Carriage," 18 *Telecommunications Policy* 435. Sec. II (1994), http://www.columbia.edu/dlc/wp/citi/citinoam11.html (accessed August 3, 2007).

[319] *Iowa v. FCC*, 218 F.3d 756,759 (D.C. Cir. 2000); *Nat'l Ass'n of Reg. Util. Comm'rs v. FCC*, 533 F.2d 601, 608-09 (D.C. Cir. 1976) (*NARUC II*), in Nuechterlein and Weiser, *Digital Crossroads*, 76, for test for common carrier. *FCC v. Midwest Video Corp.*, 440 U.S. 689, 701 (1979); *Virgin Is. Tel.*, 198 F.3d at 925, cited in Nuechterlein and Weiser, *Digital Crossroads*, 76.

[320] See various explanations cited in Cybertelecom, "Common Carriers," http://www.cybertelecom.org/notes/common_carrier.htm (accessed August 3, 2007).

[321] For a better explanation, see William Jones, "The Common Carrier Concept as Applied to Telecommunications: A Historical Perspective," http://www.cybertelecom.org/notes/jones.htm (accessed August 3, 2007).

[322] Much of this paragraph and the subsequent discussion of *Computer I* is drawn from Kevin G. Wilson, *Deregulating Telecommunications: U.S. and Canadian Telecommunications, 1840-1997* (Lanham, MD: Rowman & Littlefield Publishers, 2000), 25-40.

With the introduction of the minicomputer in the 1970s, computers became a mass-market commodity, as did the information processing power they contained. This information processing power sped the development of many communications services offered by telephone companies and other firms in conjunction with local access service, ranging from caller ID and call forwarding to access to the Internet through an ISP. Each of these enhanced communications services, whether voice or data, depends upon the information processing power of computers. The merging of computers and telecommunications presented a regulatory headache: how could regulators separate communications common carriage, which is regulated, from the information processing component, which is not regulated?[323] The need for regulation stemmed from antitrust concerns, particularly the issue of denial of (access to) essential facilities, since this the telephone system was a monopoly held by AT&T. (Common carriers provide the basic transmission and switching. In a competitive market for remote data processing, the common carrier would also provide the underlying transmission and switching to its competitor, giving it incentive to provide either lower quality or more expensive basic communications service in order to give itself an advantage. While this would not be a problem in a competitive market, since the competitor could use a different basic communications service provider, AT&T's status as a monopolist eliminated this choice and made regulation necessary to ensure competition in data processing.)[324]

Thus, the question of *where to draw the line* between computing and communications, information processing and basic communications, is critical. The decision of where to draw the line would enable regulators to decide not only what and how to regulate common carriers, but would "enable the regulator *not to regulate* the computer/data processing industry."[325]

Computer I

The beginning of an answer to this question – which due to ever-changing technologies continues to be a hotly debated question even today – began with the Computer Inquiries in 1965.

---

[323] Wilson, *Deregulating,* 151-2.
[324] Wilson, *Deregulating,* 152.
[325] *Ibid.*

The Computer Inquiries attempted to answer the question of what was data processing and what was message switching.[326] Unfortunately, it was not particularly successful.

The first Computer Inquiry (*Computer I*) evaluated hybrid services based on the notion that the amount of data processing relative to communications could be measured. The Commission's solution created a framework divided by functionality. At one end of the spectrum were regulated pure communications. At the other was unregulated pure data processing. Between the two lay the grey zone of hybrid communications and hybrid data processing, with the question of whether it was regulated or not depending on whether it was a hybrid communication, consisting of "*mostly message switching* with some incidental computing," or hybrid data processing, which is "*mostly data processing* with some incidental message switching."[327] There was no objective test to determine which function dominated, and the FCC did not offer guidelines or examples to show how it might draw the line.

Unsurprisingly, the net result was confusion and a failure to promote growth of new computer communications services, contrary to the intent of the FCC, which views its role as one of promoting technological innovation. The ambiguity meant that AT&T could not participate, since AT&T was barred from competing in unregulated sectors, despite possible economies of scale and scope that might have existed between enhanced and basic communications services. The ambiguity also discouraged enhanced services providers, who feared being regulated as common carriers. In short, the FCC had something of a 'Three Bears' experience. It had over the course of AT&T's long monopoly over communications services learned that excessive regulation discouraged innovation and competition. However, during the course of Computer I, it also learned that too little regulation, or rather too much ambiguity, also discouraged innovation by creating additional uncertainty.

Computer II

Given the general ineffectiveness of *Computer I,* the FCC initiated another computer inquiry in 1976, issuing its second decision, *Computer II,* in 1980. The most important result of

---

[326] The question of whether common carriers could be allowed to provide data processing services was answered by the "structural separation" requirement. Under this solution, the common carriers could only provide data processing through structurally separate subsidiaries that could not be represented by the parent company or use the parent company's name or symbols to market its services. This decision loosened when it was challenged by GTE, although the FCC continued to bar AT&T from providing data services under the 1956 Consent Decree. Wilson, *Deregulating,* Deregulating Telecomm, 155. See Chapter 5 and especially 6.

[327] Wilson, *Deregulating,* 157.

Computer II was the establishment of a new framework for hybrid computers-communications technologies: basic vs. enhanced services. This distinction forms the basis of the regulatory categorization that governs telecommunications today. (See Telecommunications Act of 1996 below.)

The Broadband Inquiries

The FCC's history of dealing with new technologies by seeking more information rather than necessary regulating by default extends beyond its experience with the intersection of computing and communications. The FCC, founded as a successor to the Federal Radio Commission, has dealt with a series of new technologies during the course of its lifetime. This, perhaps, has predisposed it to being aware of the changing nature of technology and sensitivity to the impact of regulation upon technological development. It may also have taught the FCC to remain attentive to new technologies coming over the horizon, with the notion that they will eventually impact the FCC's work – whether by creating new areas that require regulation, or by affecting existing regulated areas. The *Computer Inquiries* remain the best-known example of the FCC's attempt to exercise foresight with regards to emerging technologies. However, it is not the only example.

In 1968, just two years after the launch of *Computer I,* the FCC opened an inquiry into broadband services in an attempt to anticipate technical developments in cable television. Cable television operators had begun running cables into homes and business offices, and the telephone companies feared two-way cable TV would become a direct threat to the telephone business, particularly if the cable operators were able to interconnect with the PSTN. Telcos began forcing cable operators renting space on their utility poles to limit their operations to providing only entertainment television services. The FCC held hearings on the relationship between cable and telephone operators, and eventually ruled that telephone companies were not allowed to own cable television operators. (95-97)

The "Broadband Inquiry" (Docket No. 19397) began in December 1968 and culminated in an NPRM adopted on June 24, 1970 that stipulated that cable should include a "return communication capability" that provided a minimum equivalent capacity to a 4KHz message channel (bandwidth of a dedicated telephone circuit).

* Information in this box is taken from Lawrence McCray, "The Politics of Regulation: Multi-Firm Trade Associations in Telecommunications Policy-Making," (PhD idss., Massachusetts Institute of Technology, 1974), 95-98.

Computer II was also prompted by a shift in technology, caused by the trend in computer miniaturization driven by the shift from transistors to integrated circuits and then microchips. Mini computers, and later personal computers, were considerably cheaper and faster, and made the terminals intelligent, unlike the 'dumb' terminals of mainframe computers. It also created intelligent peripheral equipment and distributed computer systems. *Computer II* fully liberalized CPE, from handsets (AT&T had given up attempting to prevent subscribers from owning their

own telephones) to data terminals. It also liberalized all enhanced services, tossing the *Computer I* framework of hybrid communications vs. hybrid data processing out.

The Commission replaced the *Computer I* framework with the now-familiar categories of basic versus enhanced service. Basic service was defined as "a pure transmission capability over a common communications path that is virtually transparent in terms of its interaction with customer supplied information."[328] Basic services, such as ordinary telephone service and private lines for voice, video, and data, would be regulated. Everything that was not a basic service would be considered an enhanced service, and therefore not regulated.[329] An enhanced service was defined as one that "acted on the format, content, code, protocol or similar aspects of the subscriber's transmitted information, or provided the subscriber additional, different, or restructure information, or involved subscriber interaction with stored information."[330] Examples would include information retrieval services such as email or databases or data processing.

The distinction between basic and enhanced service applied to all common carriers. Basic communications services were still regulated under Title II of the Communications Act (1934), which dealt with common carriers. Enhanced services would be unregulated.

Computer II also opened up the market for more competition in enhanced services by allowing telephone companies to enter the market. However, in order to existing telephone companies to leverage their size or control over physical facilities and create unfair competition, the Commission required both structural separation and unbundling of raw transmission functions. Structural separation meant that the largest telephone companies, such as Bell and GTE, could only provide enhanced services through a completely separate corporate affiliate or subsidiary.[331] Unbundling meant that raw transmission functions (e.g., high speed circuits) had to be separated information services offerings (e.g., data processing). These transmission functions were to be tariffed as stand-alone "telecommunications service", purchased for the

---

[328] Second Computer Inquiry, *Final Decision*, 77 FCC2d 384, 387 (Computer II Order), 420. ("*Computer II*").
[329] Wilson, *Deregulating*, 159.
[330] *Computer II*
[331] The subsidiary had to own and locate all switching and computer equipment on own premises, and all operations (accounting, officers and personnel, marketing, advertising) had to be separate. The subsidiary was also banned from owning its own transmission facilities, and was instead required to lease them from a parent or other common carrier on a tariffed basis. Bethesda Research Institute, *Separate Subsidiaries and Structural Separation in United States Telecommunications: Conceptual Analysis, Applications, and Prognosis.* Prepared for the Ministry of Transportation and Communications, Province of Ontario by Research Studies Division, Bethesda Research Institute, Ltd. Bethesda, Maryland, 1985, in Wilson, *Deregulating*, 160.

company's own use, and sold on a non-discriminatory basis to all unaffiliated information service providers that requested it.[332]

The FCC was soon deluged with requests for waivers. "Although the structural separation requirements were designed to prevent unfair competition, this was not their ultimate purpose. In this case, competition was not an end in itself. Rather it was a means to promote innovation and the introduction of new services... The ultimate test of *Computer II* would be whether new services became available to the public. If the FCC denied AT&T's application, and no other firm stepped in to offer the service in its place, then the *Computer II* rules were not meeting their objective."[333]

AT&T divestiture and Computer III

The divestiture of AT&T occurred just as the FCC was evaluating the effects of *Computer II.* The settlement of the antitrust suit brought against AT&T by the Department of Justice (DOJ) resulted in the breakup of the Bell monopoly. The breakup separated the theoretically competitive parts of the Bell system, the long distance services, from the parts considered to be natural monopolies, the regional Bell Operating Companies (BOCs). The divestiture had two important consequences for VoIP. First, the divestiture opened up the market for competition and innovation, which arguably allowed for the development of VoIP. Second, the divestiture set the stage for the creation of the extremely convoluted access charge regime that exists today. Although cross-subsidization of local and rural service by long distance and urban or corporate subscribers had existed for decades, it was less important in the days of the Bell monopoly. The access charges that constitute a large proportion of local exchange carriers' income became much more important once the payer and payee were no longer part of the same company.

---

[332] Nuechterlein and Weiser, *Digital Crossroads*, 153. Nuechterlein and Weiser point out that the *Computer II* unbundling requirement is different from the *facilities* unbundling requirement in the 1996 Telecommunications Act, which requires telephone companies to lease *facilities* or capacity on those facilities, and not the transmission service itself. However, as Nuechterlein and Weiser note, "at the margins the two concepts merge, because leasing capacity on network facilities is often functionally equivalent to providing a transmission service over those facilities." See footnote, 560.

[333] Wilson, *Deregulating*, 160.

*** The rest of this section can be skipped by readers not interested in the legal and regulatory details of the divestiture. It contains further details of how the AT&T divestiture set up the regulatory and industry structure that currently affects VoIP. ***

When the Department of Justice filed its antitrust suit against AT&T, AT&T had existed for more than a century, most of it as a regulated monopoly. However, by the 1970s, newly formed competitors and regulators alike were beginning to question the value of AT&T's monopoly and its impact on consumer welfare and innovation. MCI had just won an antitrust lawsuit against AT&T in 1981 when *United States v. AT&T* went to trial. The suit was settled in January 1982, with AT&T agreeing to the divestiture of the regional BOCs, sometimes called the Baby Bells.

In theory, the settlement separated the parts of AT&T that constituted natural monopolies, the BOCs, from those parts of AT&T that were potentially competitive, the long distance service. The separation was not only functional but structural: the Baby Bells would be entirely independent companies. They became what we now call local exchange carriers (LECs).[334] Under the settlement, the constraints of the 1956 consent decree would also be lifted, allowing AT&T to enter into the information services market. The BOCs would be local operating companies. Because they were considered natural monopolies, they would not be permitted to enter the long distance, information service or manufacturing markets. They would also be required to provide equal access to any long distance company. In other words, they were to act

---

[334] Telecom regulation has its alphabet soup tendencies. LECs come in two varieties: incumbent LECs (ILECs, pronounced "eye-leck") and competitive LECs (CLECs, pronounced "see-leks"). The best-known and largest ILECs are the regional BOCs: Verizon, SBC, Bell South, and Qwest. There used to be seven regional Bells, but due to consolidation, there are now only four. Verizon is a combination of Bell Atlantic and NYNEX, plus the non-BOC GTE. SBC is a combination of Southwestern Bell, Pacific Telesis, Ameritech, and the non-BOC Southern New England Telephone. Qwest purchased US West in 2000, thus inheriting its regulatory obligations. There are hundreds of other CLECs as well. Many of these are in rural areas, and were independent carriers that were never part of the Bell system. Some are "rural" carriers.
There are also many CLECs. These include the traditional long distance companies AT&T and MCI (formerly WorldCom), as well as newer firms such as Covad Communications, which leases lines from incumbents to provide high speed Internet access. CLECs tend to serve two very different types of customers: enterprise customers and mass market customers. Enterprise customers are large businesses, often with multiple offices, that generate huge amounts of data and voice traffic (e.g., Merrill Lynch). These customers are connected directly to the CLEC's network using fiber optic transport pipes, which may either be owned outright or leased from ILECs. These customers were some of the earliest adopters of VoIP technologies, although most still use Class 1, or phone-to-phone VoIP. Mass market customers, the second category of customer, are smaller business and residential subscribers. This category is probably more familiar to the general reader. They purchase local and long distance service from the CLECs, which provide the service by leasing local facilities from ILECs at regulated rates. Nuechterlein and Weiser, *Digital Crossroads*, 76-79.

as common carriers. The Modified Final Judgment (MFJ) was entered on August 24, 1982, and the divestiture took place on January 1, 1984.[335]

Unfortunately, the nature of the divesture agreement and implementation also created a divide in telecommunications regulation. The agreement initially negotiated by the Department of Justice (DOJ) and AT&T was modified by Judge Harold Greene of the Federal District Court for Washington, D.C.. Greene had determined that he would continue to oversee the implementation of the Modification of Final Judgment in his court, which included a clause prohibiting BOCs from providing information services, defined as "the offering of capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information which may be conveyed via telecommunications" (*Modification of Final Judgment. United States v. AT&T,* 522 F. (D.D.C. 1982), IV. J). The MFJ essentially limited the BOCs to providing only basic common carriage at the local level. However, the existence of the MFJ also meant that there were two jurisdictions for filing of waivers. The DOJ continued to play a role in policy setting through the triennial review of the MFJ.[336]

The two separation frameworks, with two different administrative authorities, left much confusion concerning the role that BOCs should play in the provision of new services. Adding to the confusion was the fact that restrictions on providing information services (MFJ) and enhanced services (*Computer II*) were not interpreted to mean the same thing. It was also uncertain whether the FCC or the Court's jurisdiction should take precedence.[337]

Meanwhile, the FCC had come to the conclusion that structural separation requirements were not an effective basis for policy, and were indeed an obstacle to innovation and new services. As the Commission stated in 1986:

> "We conclude that the record strongly supports a finding that the inefficiencies and other costs to the public associated with structural separation significantly outweigh the corresponding benefits.... The relative costs and benefits of the structural separation requirements now imposed on the enhanced services operations of AT&T and the BOC's, compared with the costs and benefits of non-structural safeguards designed to service the same regulatory goals, lead us to conclude that the structural separation requirements should be eliminated.[338]

---

[335] History taken from AT&T, "History," www.att.com/history (accessed August 3, 2007); Cybertelecom, "AT&T AntiTrust," http://www.cybertelecom.org/notes/att_antitrust.htm#ant3 (accessed August 3, 2007).
[336] Wilson, *Deregulating*, 161
[337] Wilson, *Deregulating*, 162.
[338] FCC 1986, quoted in Stuart Brotman, *The Telecommunications Deregulation Sourcebook.* (Boston: Artech House, 1987), quoted in Wilson, *Deregulating,* 162.

The solution the FCC eventually settled upon in *Computer III* was to allow BOCs to integrate enhanced services with their other operations as long as they allowed outside providers of enhanced services equal access to local networks. This was made possible through a program called Open Network Architecture (ONA). In the short-term a framework called Comparably Efficient Interconnection (CEI) was used, but CEI was a temporary measure, pending approval by FCC of comprehensive ONA plans that BOCs are required to file with FCC. What this provided was a stopgap measure that ensured that competitive providers of the same service had 'equivalent access' to the BOC's network capabilities.[339] The ONA designated a new way of organizing the relationship between LECs and providers of enhanced services at the technical and organizational levels by providing for unbundling of services – dial tone, switching, ring/ busy tones, etc. All of these Basic Service Elements (BSEs) had to be offered to enhanced providers on a tariffed basis, with tariffs to be approved by the FCC. In other words, what the FCC required was that BSEs be offered a la carte to enhanced service providers so that they could combine them with additional components to make new services. "ONA was conceived by the FCC to be an evolutionary process, not a static set of network functions. It was meant to change and evolve in conjunction with changes in technology, specifically switching technology."[340]

The AT&T divestiture had far-reaching consequences for the telecommunications industry and for VoIP. I will only focus on a few that pertain to current VoIP regulation here. First, it opened up the field to competition in long distance services. One of the major motivations behind the development of VoIP and its adoption by early users was the high cost of long distance calls – especially international calls – since VoIP calls are free or almost free. Second, the fragmentation of AT&T into the regional Bells set the stage for the rise of today's crazy-quilt access charge regime. The question of who must pay which rates to whom is a central question in the regulatory battle over VoIP, even if the FCC has thusfar taken little action to settle the debate. The overnight creation of the Baby Bells and the mushrooming of assorted other telecom players no longer under the Ma Bell umbrella meant new actors with different interests could find arbitrage opportunities to exploit in the convoluted access charge regime. The fact the various companies were now independent – or never part of – Ma Bell just makes

[339] Wilson, *Deregulating,* 162.
[340] Wilson, *Deregulating,* 163.

the stakes in the cross-subsidy game considerably higher than when all companies were part of the AT&T family.

Communications Assistance for Law Enforcement Act (CALEA 1994)

The driving force behind the FBI's push for CALEA was the fear that the shift to digital telephony (digital exchange switches) would make it more difficult or even impossible to tap phones at the central office. As the origins of CALEA have already been discussed in the chapter on cryptography, here I will only briefly summarize the obligations, putting more emphasis on the technical difficulties and security and economic implications of imposing CALEA obligations upon VoIP providers. VoIP did not exist as any sort of commercial alternative to telephony when CALEA was passed. To date, the FCC has imposed CALEA obligations on facilities-based broadband Internet access providers and interconnected VoIP, meaning VoIP that connects to the PSTN (Class 2).

CALEA requires telecommunications carriers and manufacturers of telecommunications equipment to design or modify their equipment to ensure that they can accommodate law enforcement wiretaps without the subject of the wiretap being aware of the wiretap. CALEA also requires that call detail records (the pen register) be made available to law enforcement. Call detail records include information such as the identities of call origin and endpoint, duration of call, and amount billed for the call. Meanwhile, the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which established the rules for obtaining wiretap orders,[341] and the Electronic Communications Privacy Act (ECPA) of 1986, which extended government restrictions on wiretaps to computer data transmissions,[342] require that all wiretaps must protect security and privacy (of communications other than those by the subject of the wiretap).

Problems Applying CALEA to VoIP

The two major technical problems in applying CALEA to VoIP are *mobility* and *identity* verification.[343] VoIP mobility is both one of the most appealing features of VoIP as well as the

[341] Public Law 90-351, June 19, 1968, 82 Stat. 197, 42 U.S.C. §3711. This act established the Law Enforcement Assistance Administration and established the rules for obtaining wiretap orders.
[342] Electronic Communications Privacy Act, 18 U.S.C. §2510 (1968), amended by Public Law 99-508, 100 Stat. 1848 (1986). ("ECPA").
[343] The summary of technical, economic, and security difficulties/ implications of applying CALEA to VoIP are drawn from Steven Bellovin, Matt Blaze, et al, "Security Implications of Applying the Communications Assistance

biggest obstacle to successful CALEA implementation. Wiretaps as applied to traditional telephone networks are relatively simple. The centralized and fixed nature of the telephone network makes the central switch the obvious location for the wiretap, because fixed phone numbers are served by fixed switches. (Incoming calls for cellular phones are also served by readily identifiable switches.) VoIP, on the other hand, has neither of these features. First, because VoIP runs over the Internet, the equivalent of the switch is a router. However, packet-switched communications do not necessarily follow a fixed route, so determining where to put the wiretap is difficult.[344] In addition, the router is not necessarily owned by a specific carrier, which further complicates placement of the wiretap. Second, the IP address of the targeted VoIP user is not necessarily fixed. Unlike a telephone number, the VoIP user could be using a series of dynamically assigned IP addresses, as would occur in a hotel lobby, coffee shop, or other wireless hotspot.

Even assuming that a VoIP provider can guide the targeted caller's communications through a LEA-controlled point at which the tap can be installed, there are other issues as well. First, because legal jurisdiction is assigned geographically, the switch (router) must be under the jurisdiction of the authority that authorized the wiretap. Second is a technical issue: the switch operator needs to receive real-time (authenticated) messages ordering them to start and stop the wiretap, since most message will probably be of short duration, in order to comply with the *minimization* requirement of the ECPA. That is, the tapped communications can only be those of the targeted party for the targeted topic.[345] Violating the minimization requirement would mean widescale wiretapping of non-target individuals, which in addition to being a violation of their privacy, would create a significant public backlash and drop in support for use of wiretapping. Although not quite equivalent, a measure of the possible hostile reaction can be seen in the

---

to Law Enforcement Act to Voice over IP", paper for the Information Technology Association of America, http://www.itaa.org/news/docs/CALEAVOIPreport.pdf (accessed August 3, 2007).

[344] To continue the analogy from the first section of this chapter, remember that a packet is like a car trying to get from Fenway to MIT. A wiretap is like a person trying to intercept that car. Imagine that the bridges over the Charles River are routers. Now, since in packet-switching there is no way to know a priori whether the car will be driving over the Harvard Bridge, the BU bridge, or the Longfellow Bridge, it is not necessarily clear where the person trying to intercept the car should stand. Just to complicate matters, remember again that the various cars (packets) can each take separate routes, so a tap on the Harvard Bridge may only intercept some of the cars, which translates as only part of the message.

[345] That is, when tapping one individual in the household, the wiretap must not also tap the communications of everyone else living in the household. In addition, if the wiretap is for communications pertaining to, say, money laundering, communications regarding other topics cannot be tapped.

public outcry over the NSA's unauthorized wiretapping scandal in the past two years.[346] The third issue is both social and economic: of the approximately 1500 ISPs in the U.S., most are small, with fewer than 100 employees.[347] The switch operator would need to feel legally comfortable complying with the wiretap order. Perhaps more troublesome, the ISP would need to have the resources (financial, physical, manpower, technical capability) to support real-time wiretapping. Given the small size of most ISP, this could post a significant financial burden that might drive the ISPs out of business.

The second technical issue in applying CALEA to VoIP is identity verification. With wiretap orders on traditional telephony, usually a telephone number is specified.[348] The wiretap order could be issued against a specific person. However, on the Internet a single person may have multiple identities—multiple email addresses, for example, or in this case, multiple VoIP accounts (possibly with multiple providers). As the *New Yorker* cartoon put it, "On the Internet, nobody knows you're a dog." There is also a Catch-22: even if a specific call is targeted, given the nebulousness of Internet identity, it is difficult to know who is actually making the call without having access to the call. (Granted, this is also a problem for traditions POTS telephony.)[349] The pen register information is not particularly useful, since anyone could be using the target's VoIP identity (username). In addition, if the tap is on the call recipient's end, LEA must be able to determine when calls are from a specific person – not easily done, since all packets basically look the same.

More broadly, applying CALEA to VoIP may require intercept design features that weaken the security of the Internet application space as a whole. Because dynamic routing on the Internet means the path any given packet will take is unpredictable, comprehensive VoIP intercept capability requires the cooperation of a significant portion of the routing infrastructure. Voice packets are largely indistinguishable from packets carrying other communications or data, so CALEA requirements would most likely have to be implemented in such a way that covers all

---

[346] See, for example, The Washington Post's online feature on the NSA warrantless surveillance issue, with links to archived articles and editorials, at http://www.washingtonpost.com/wp-dyn/content/linkset/2006/02/03/LI2006020301869.html.

[347] OneSource, *High-technology Product Code; internet infrastructure services (U.S. only),* run 27 April 2006, in Bellovin, "Security Implications," 14.

[348] On occasion, the telephone number is not specified, as with a roving wiretap order. Roving wiretap orders are usually for situations such as a bank of payphones.

[349] Thanks to David Clark for reminding me of this point.

Internet communications.[350] This type of intercept capability would require inserting intelligence into the middle of the network, which runs contrary to the design principle of the Internet. (Dumb network, intelligence at the end nodes)

In 2000 the IETF Network Working Group actually "declined to consider wiretapping requirements as part of the standards process... because of the potential security problems involved. Various attacks, including man-in-the-middle alteration of data (done by attacker interposed between the communication endpoints), capture of identity information and passwords, and many other pernicious behaviors could well be enabled by CALEA-like accommodations."[351] Also, since CALEA requirements only apply to U.S.-based applications, it could harm U.S. business both by imposing the costs of CALEA compliance and driving traffic to non-U.S.-based locations who are not subject to CALEA. (Alternatively, end-to-end encryption or tunneling could allow users to circumvent intercepts while still utilizing U.S.-based services.) In addition, it could actually harm national security, as routing communications out of the U.S. "would destroy certain advantages currently enjoyed by U.S. intelligence."[352]

ACTA Petition 1996

The FCC confronted VoIP as a policy issue for the first time in March 1996. The Carriers Telecommunication Association (ACTA), an industry comprised primarily of small to medium-sized resellers of long-distance services, filed a petition with the FCC requesting a Ruling, Special Relief, and Institution of a Rulemaking relating to interstate and international VoIP.[353] The VoIP in question in this petition was IP-to-IP VoIP, such as the products produced by VocalTec, one of the offending parties named in the petition.[354] The FCC's Public Notice states:

> "ACTA alleges that providers of "Internet phone" software and hardware are operating as uncertified and unregulated common carriers, in contravention of FCC rules, and seeks three forms of relief. First, ACTA seeks a declaratory ruling establishing the Commission's authority over interstate and international telecommunications services using the Internet. Second, ACTA asks the Commission for special relief: to order named and unnamed respondents immediately to

---

[350] Bellovin, Blaze 13.
[351] *Ibid.*
[352] *Ibid.*.
[353] Emir A. Mohammed, "The Growth of Internet Telephony: Legal and Policy Issues," *First Monday* http://www.firstmonday.org/issues/issue4_6/mohammed/index.html#m3 (accessed August 3, 2007).
[354] Petition, In the Matter of the Provision of Interstate and International Interexchange Telecommunications Service via the "Internet" by Non-Tariffed, Uncertified Entities," http://www.fcc.gov/Bureaus/Common_Carrier/Other/actapet.html (accessed October 28, 2007).

> stop provisioning Internet phone software and hardware without complying with the regulatory requirements of the Communications Act of 1934. Finally, ACTA urges the Commission to initiate a rulemaking proceeding to consider rules governing the use of the Internet for the provision of telecommunications services."[355]

In other words, ACTA anticipated that IP-to-IP VoIP, a low- to no-cost alternative to long distance telephony, represented an emerging threat to its members' bottom line. ACTA therefore sought to leverage the FCC's regulatory authority to abolish the threat altogether. That is, it wanted the Commission to ban Internet telephony altogether, but if not, then to force VoIP providers to comply with the intercarrier compensation regime.[356] Although the FCC put the petition up for comment, and received quite a few in opposition, the Commission never acted on the petition.[357] In 1998, the FCC noted in the Stevens Report that the petition was still pending.[358] This suggests that the delay, including forbearance from imposition of access charges, was a deliberate move by the FCC intended to allow VoIP technology to mature and innovation to continue unentangled by legacy regulation, per statements in the Stevens Report and subsequent OPP working papers.[359] (See below.)

It is not actually clear what the status of the ACTA petition is. ACTA merged with Comptel in early 1999, but it seems that Comptel neither pursued nor withdrew the petition.[360] The one thing the ACTA petition did accomplish, however, was to prompt the formation of an influential pro-VoIP industry interest group, the VON Coalition (Voice on the Net).[361]

Telecommunications Act of 1996[362]

For purposes of this dissertation, there are four items in the Telecommunications Act of 1996 that are important. First, the Act revised and codified the dual categories of telecommunications service and information service. The former category is regulated; the latter

---

[355] Public Notice, Common Carrier Bureau Clarifies and Extends Request for Comment on ACTA Petition Relating to "Internet Phone" Software and Hardware, 12 FCC Rcd 15982 (March 25, 1996), http://www.fcc.gov/Bureaus/Common_Carrier/Public_Notices/1996/da960414.txt (accessed August 3, 2007).
[356] In a personal communication with David Clark, he pointed out that in other countries such as Turkey, VoIP was banned in order to preserve the state postal telegraph and telephone (PTT) monopoly. It is worth exploring in future research whether the U.S.'s lack of a state-run or state-sanction monopoly may help account for the lack of a ban on VoIP in the U.S. (David D. Clark, personal communication, December 21, 2007.)
[357] Cybertelecom, "ACTA Petition," http://www.cybertelecom.org/voip/acta.htm (accessed August 3, 2007).
[358] *Stevens Report*, footnote 172.
[359] See links to various articles on ACTA at Cybertelecom, "ACTA Petition."
[360] Cybertelecom, "ACTA Petition."
[361] *Ibid.*
[362] Telecommunications Act of 1996, 47 U.S.C, 151, Public Law No. 104-104, 110 Stat. 56 (1996).

is unregulated. Therefore, the characterization of VoIP as one or the other determines whether VoIP is subject to legacy regulations. Second, the Act retained the statutory "silos" from the 1934 Act, thus perpetuating the assumption that services and facilities will be permanently linked. This assumption is blatantly untrue for Internet-based technologies, which are agnostic to physical media. Therefore, the statutory silos limit the Commission's ability to regulate Internet technologies such as VoIP in a manner consistent across platforms. Third, the Act grants the Commission enormous regulatory discretion, including the right to "forbear" from applying almost any provision of the Act. However, as some telecommunications scholars have noted, the Commission may not be politically or organizationally capable of effectively exercising this discretion. Fourth, the Act established the universal service fund, a new mechanism for subsidizing telephony in rural, insular, and high cost areas.

The Telecommunications Act of 1996 was the most important telecommunications legislation since the New Deal. (See Communications Act of 1934.) Unfortunately, it is also widely regarded as one of the densest pieces of legislation ever written – not to mention already outdated by the time it had passed into law.[363] (The law largely failed to take into account the Internet.) As Supreme Court Justice Antonin Scalia wrote, "It would be gross understatement to say that the 1996 Act is not a model of clarity. It is in many important respects a model of ambiguity or indeed even self-contradiction. That is most unfortunate for a piece of legislation that profoundly affects a crucial segment of the economy worth tens of billions of dollars."[364]

One of the major flaws of the Act was that it did not foresee the huge impact that the Internet would have on telecommunications. The Act renamed and slightly revised the "basic" vs. "enhanced" distinction between types of services in telecommunications discussed in *Computer II.* For all intents and purposes, "telecommunications" is basic service; "telecommunications service" is basic service offered at common carriage; and "information service" is enhanced

[363] Nuechterlein and Weiser, *Digital Crossroads*, 69.
[364] *AT&T Corp. v. Iowa Utilities Board*, 525 U.S. 366, 397 (1999), in Nuechterlein and Weiser, *Digital Crossroads*, 69.

service.[365] As a broad generalization, telecommunications services are regulated, and information services unregulated (or rather, less regulated).[366]

Formally, a "telecommunications service" is defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[367] "Telecommunications" is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[368] An example is traditional telephone service, without add-ons such as voice mail or caller ID. "Information service" is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service."[369] Examples of information services include Internet access service, computer bulletin boards, voicemail, and directory services.

These definitions, as alluded to in previous sections, are the source of quite a few regulatory problems. First, the definition of "telecommunications" in the 1996 Act is not the same one as in CALEA. The problems this raises will be discussed in the next section, in conjunction with the Joint Petition to apply CALEA to VoIP. Second, the definitions do not necessarily fit neatly with Internet-based technologies. The characterization of VoIP is important, however. Anything characterized as a "telecommunications service" triggers all of the obligations that accompany any telecommunications service (such as all of the common carriage provisions of traditional telephony). (Section 4 will discuss several of these as they apply to VoIP.)

---

[365] Nuechterlein and Weiser, *Digital Crossroads*, 152. See 47 U.S.C. § 153(43), (46), (20); First Report and Order, *Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934,* 11 FCC Rcd 21,905, ¶ 102 (1996), *modified,* 12 FCC Rcd 2997 (1997), 12 FCC Rcd 8653 (1997), *aff'd, Bell Atl. Tel. Cos. v. FCC*, 131 R.3d 1033 (1997); *Stevens Report.*

[366] This is a generalization. Both types of service are regulated. Telecommunications service just happens to be much more heavily regulated due its common carrier roots, so information services are usually called "unregulated".

[367] 47 U.S.C. 151 §51

[368] 47 U.S.C. 151 §48

[369] 47 U.S.C. 151 §41

Two of the three classes of VoIP have been characterized by the FCC. The remaining one, Class 2 (IP-to-PSTN) VoIP, has characteristics of both telecommunications service and information service, which makes characterization difficult. The FCC defined IP-to-IP VoIP as an unregulated information service in the *Pulver Order* on the grounds that pulver.com's Free World Dialup service did not provide transmission capabilities nor charge a fee. (Both of these are required for a service to be characterized as "telecommunications.") The FCC also categorized "phone-to-phone" long distance service, a Class 1 VoIP service, as telecommunications in a ruling in 2002. AT&T had petitioned to have its phone-to-phone service declared an unregulated information service, but the FCC ruled against it on the grounds that no net conversion took place. (AT&T's service originated and terminated on the PSTN, but traveled over an IP backbone in the middle, which required conversion into and then back out of IP packets.) Class 2 services such as Vonage seem to fall somewhere in between the two. Many of Vonage's characteristics seem to suggest it is a telecommunications service. For example, Vonage charges a fee for its services; dropping Vonage-initiated calls onto the PSTN requires net protocol conversion; and Vonage users have NANP telephone numbers. On the other hand, Vonage does not provide transmission functions, which would seem to be a key component of being a telecommunications service. (Remember that Vonage users must supply their own broadband connections.) Therefore, it is not quite clear which category Class 2 services like Vonage fall.

The 1996 Act also created or perpetuated other technology-regulation incompatibilities. The Act left intact the statutory "silos" established in the 1934 Communications Act, which assumed that services and facilities would always be closely associated. (e.g., Title II is wireline telephone companies subject to common carrier regulation; Title III is broadcast, or use of the airwaves for TV or cellular telephony; Title VI is cable services) The Internet, and the applications like VoIP that ride on it, do not conform to these neat categories.[370] The Internet has a horizontal, or "layered" architecture that does not depend on the physical layer that carries it. A packet does not care whether it is transported over a cable wire, wirelessly through the air, or on a telephone network. Neither does it matter whether a packet is carrying voice, video, audio, text, or any other service. That determination is a function of the higher-level application that rides on

[370] Actually, VoIP can ride on any IP-based, packet-switched network, whether it be a private IP network or the Internet. For shorthand, however, I will simply refer to the "Internet".

top of the transport layer, with processing done by the end node (the user's computer) and not the network.

One of the results of leaving these silos intact is Congress failed to set forth a regulatory framework for broadband. Congress did not forsee that cable and telephone companies would compete in the market for broadband Internet access. Admittedly, the market barely existed in 1996 when the Act was passed. Until then, cable companies had largely ignored the telephone market, since upgrading their systems to provide ordinary circuit-switched services generally exceeded expected revenues, especially since many residential customers were paying subsidized, below-cost rates. Meanwhile, the copper telephone wires into most homes did not have sufficient bandwidth to be a competitive alternative to cable TV service.[371] Unfortunately, this regulatory ambiguity also means that there is no way to "ensure regulatory parity between... competing platforms."[372] This has resulted in many of these decisions being made or appealed in the courts, most notably in the *Brand X* decision.[373]

To compound the problems the ambiguous language of the Act presented, Congress granted the Commission enormous discretion in how to interpret and apply the various provisions of the Act. In theory, Congress delegates rulemaking authority to administrative agencies because the agencies possess expertise and institutional flexibility that Congress lacks. In other words, Congress expects the agencies to be able to adjust to new conditions, such as changing technologies, faster than Congress' notoriously slow process. [374] This is probably true

---

[371] Nuechterlein and Weiser, *Digital Crossroads*, 73.

[372] *Ibid.* 73.

[373] *Brand X* was at its core a suit over the classification of cable services. Because cable and wireline telephony are governed under two different Titles of the 1996 Telecommunications Act, cable companies are not subject to many of the regulations telephone companies must follow. Brand X argued that cable services are telecommunications services, and cable providers are common carriers. Defined as such, they should be subject to the requirements of common carriage, including the requirement to lease their facilities at tariffed rates to ISPs. The first court had ruled against Brand X, which appealed the decision. In an effort to preempt the Circuit Court's decision, the FCC issued a ruling stating that cable services are information services. The 9th Circuit Court, on appeal, agreed with Brand X, and ruled that cable services are a combination of both telecommunications and information services, and therefore, as per an earlier case (*AT&T v. City of Portland*, 216 F.3d 871 (2000)), subject to the regulatory requirements of both. The cable company appealed to the Supreme Court, which reversed the ruling (in part) and decided that cable is not a telecommunications service. See http://news.zdnet.com/2100-6005_22-5764187.html for an excellent summary of the case. See http://www.law.cornell.edu/supct/html/04-277.ZS.html for the Supreme Court decision.

[374] See, for example, Sheldon Kamieniecki, *Corporate America and Environmental Policy: How Often Does Business Get Its Way?* (Palo Alto: Stanford University Press, 2006), 104; Joe Bowersox, *The Moral Austerity of Environmental Decision Making: Sustainability, Democracy, and Normative Argument in Policy and Law* (Duke University Press, 2002), 27; David Epstein and Sharyn O'Halloran, *Delegating Power: A Transaction Cost Politics Approach to Policy Making under Separate Powers* (Cambridge: Cambridge University Press, 1999); Edwin Meese

in a comparative sense. No matter how slow, or how inept the FCC may or may not be, they are almost certainly more agile and expert than Congress. In the case of the FCC, there is no doubt about their technical expertise. Administratively and organizationally, however, the FCC has many features that make it somewhat inefficient.[375]

Quite a few telecom experts, including supporters of the FCC, have argued that the FCC as an agency is not optimally designed to regulate telecommunications effectively. First, it is a multi-headed organization set up to rule by committee. The Commissioners are politically appointed and politically affiliated, deliberately selected to maintain a balance in favor of the party in the White House. Second, the Commission is vertically divided into bureaus and offices that do not necessarily correspond with technology or industry structure. Third, the Commission shares jurisdiction over telecommunications policy with the states, the Federal Trade Commission, and the federal courts.[376] None of these characteristics is conducive toward effective or efficient policy-making.

---

and David F. Forte, eds., *Heritage Guide to the Constitution* (Regency Publishing, Inc., 2006); Alec Stone Sweet and Mark Thatcher, *The Politics of Delegation* (Routledge, 2004).

[375] Nuechterlein and Weiser, *Digital Crossroads*, 419.

[376] Alfred Kahn, the regulatory economist, occasional consultant to the Bell companies, and person perhaps most responsible for the abolition of the Civil Aeronautics Board and airline deregulation, writes that assigning the FCC responsibility for ensuring "access by challengers to essential network facilities at reasonable rates presents them with a temptation... to micromanage the process of deregulation itself." He argues that the FCC has given in to that temptation, to the detriment of consumer welfare. Alfred Kahn, *Letting Go: Deregulating the Process of Deregulation* (Institute of Public Utilities and Network Industry, 1998), 70, quoted in Nuechterlein and Weiser, *Digital Crossroads*, 408.

Associate Justice Stephen Breyer of the U.S. Supreme Court has written that the "FCC systematically thwarts the cause of *competition*, at least in wireline regulation, by focusing too heavily on the needs of individual *competitors*." *Verizon Communications Inc. v. FCC*, 535 U.S. 467, 539 (2002) (Breyer, J., dissenting), quoted in Nuechterlein and Weiser, *Digital Crossroads*, 408; *AT&T v. Iow Utils. Bd.*, 525 U.S. 366, 413 (1999) (Breyer, J., dissenting); Stephen G. Breyer, *Economic Reasoning and Judicial Review* (American Enterprise Institute Press, 2004), 8-10, http://www.aei.brookings.org/admin/authorpdfs/page.php?id=840 (accessed January 12, 2008).

Even Nuechterlein and Weiser, who argue that the "FCC will remain, for better or worse, the least problematic institute to oversee the development of competition in telecommunications markets, at least for the foreseeable future," (409), point out that:

* "the FCC has long displayed a regrettable tendency to string out its decisions on important matters" despite repeated admonitions from the D.C. Circuit Court, where most appeals of FCC Orders are filed (419)
* the fact the FCC has five members, of different political parties, each subject to Congressional confirmation, means that they "may worry more about pleasing their separate constituencies within Congress or the industry than about pleasing the White House. This is a recipe for internecine intrigue and deliberative inefficiency." (Nuechterlein and Weiser, *Digital Crossroads* (420)
* the fact that "[a]ny final order of the FCC is subject to judicial review in a federal court of appeals.... [which] contributes to the indeterminacy of telecommunications regulation, particularly when undertaken by activist generalist courts that consider themselves equally equipped as specialist agencies to understand the complexities of this industry." (421)
* the fact decision-making authority is shared vertically with state regulatory agencies and also with other federal agencies significantly complicates regulation (422-3)

The regulatory flexibility Congress grants in the Act is particularly notable in the section on regulatory forbearance. The text of this section reads as follows:

> "the Commission shall forbear from applying any regulation or any provision of this Act to a telecommunications carrier or telecommunications service, or class of telecommunications carriers or telecommunications services, in any or some of its or their geographic markets, if the Commission determines that--
>
> (1) enforcement of such regulation or provision is not necessary to ensure that the charges, practices, classifications, or regulations by, for, or in connection with that telecommunications carrier or telecommunications service are just and reasonable and are not unjustly or unreasonably discriminatory;
>
> (2) enforcement of such regulation or provision is not necessary for the protection of consumers; and
>
> (3) forbearance from applying such provision or regulation is consistent with the public interest."

The Act further states that in making the determination whether to forbear,

> "the Commission shall consider whether forbearance from enforcing the provision or regulation will promote competitive market conditions, including the extent to which such forbearance will enhance competition among providers of telecommunications services. If the Commission determines that such forbearance will promote competition among providers of telecommunications services, that determination may be the basis for a Commission finding that forbearance is in the public interest."[377]

In short, the Act grants the Commission the authority to *not* impose regulation if it believes it is not necessary to promote competition. This provision is especially important for VoIP, as it is another justification for the FCC not regulating Internet and VoIP technologies, as we will see in the discussion of the two OPP working papers below.

The fourth importance feature of the 1996 Act, for VoIP purposes, was that it established a new and additional method of subsidizing rural telephone service called universal service. A major objective of the Act was to maintain low-priced local telephone service for residential

---

* "the Commission often seems more adroit at jury-rigging intellectually sloppy deals to appease industry factions in the short term than at making the analytically sound but politically difficult policy choices needed to promote long-term economic efficiency." (426-7) I cannot resist the quote Nuechterlein and Weiser cite from Judge Richard Posner, describing one FCC regulatory scheme as a set of "unprincipled compromises of Rube Goldberg complexity among contending interest groups viewed merely as clamoring suppliants who have somehow to be conciliated." (*Schurz Comm., Inc. v. FCC*, 982 F.2d 1043, 1050 (7th Circuit 1992).)

* the organization of the FCC into formal bureaus and offices corresponding to the industry segments set out in the now obsolete 1934 Communications Act puts them into vertical silos that are not necessarily in accord with how telecommunications technology (or industry segmentation) actually looks now. Current technologies, like VoIP, may actually fall under more than one bureau – particularly as VoIP moves from being confined to wired services to VoIP over wireless VoIP phones (like cell phones that run on wireless Internet connections instead of cellular towers). The organizational structure, write Nuechterlein and Weiser, "invites parochialism and occasionally outright protectionism." (Nuechterlein and Weiser, *Digital Crossroads*, 427)

[377] 47 U.S.C. 151 §401

customers in sparsely populated areas while still promoting competition. This policy is a continuation of the nearly century-old federal policy of using revenues and charges from densely populated urban areas and corporate customers to cross-subsidize rural areas that are costly to serve due to lack of economies of scale. Unfortunately, promoting competition and ensuring inexpensive rural service are not always reconcilable goals.

Due to economies of scale, competitive providers tend to seek richer, more densely populated markets. In the past, captive business customers and others paid above-cost rates that functionally subsidized rural customers. These customers, however, are the ones most likely to be poached by new competitors. Losing these customers destroys the source of the cross-subsidies from the ILECs, leaving them to serve only the costly, unprofitable customers. This would leave the incumbents with two unpleasant options: going bankrupt or raising rates. Neither of these would be politically palatable. Therefore, Congress came up with a third solution: the Universal Service Fund.[378] The universal service fund (USF) operates as a federally administered subsidization system. Carriers contribute on the basis of their retail interstate revenues, and the federal administrator then redistributes that money as subsidies to other carriers, generally those in sparsely populated areas with higher costs of (providing) service, to ensure "affordable" and "reasonably comparable" rates throughout the country.[379] As discussed in the next section, the question of whether VoIP providers must contribute to the USF – in other words, if they should be taxed as traditional telephone companies – was one of the questions the Commission faced in regulating VoIP.

Office of Plans and Policy Working Papers
Werbach (1997)[380]

The roots of some of the FCC's deliberate efforts to delay regulating VoIP can be found in Werbach's paper, although it certainly did not follow all of his recommendations. Werbach argues that the government should avoid unnecessary interference in the Internet's development. He urges the Commission not to impose legacy regulation on the Internet without careful thought, lest it produce unforeseen and unintended consequences,

---

[378] See 47 U.S.C. §254

[379] 47 U.S.C. §254; Nuechterlein and Weiser, *Digital Crossroads*, 74.

[380] I apologize in advance for quoting so much of this paper directly. This paper is possibly the best-written and most elegantly argued paper I have read on VoIP during the course of my research. Attempting to paraphrase and summarize actually detracts from the intellectual points Werbach makes.

which accords with the FCC's failure to regulate VoIP until 2004. Lastly, he makes a strong case against granting the ACTA petition.

Werbach's paper is an eloquent argument for restraint, caution, and sensitivity to the unintended consequences of regulation on the development of the Internet, technological innovation, and competition within the telecommunications industry. He believes that establishment of a level playing field, avoiding unnecessary interference in the Internet's development, and promoting competition rather than regulation will result in innovation that produces new technologies that create "new forms of competition, valuable services for end users, and benefits to the economy."[381] He states that "Government policy approaches toward the Internet should therefore start from two basic principles: avoid unnecessary regulation, and question the applicability of traditional rules."[382]

With respect to existing FCC regulatory and statutory requirements, Werbach "recommends that government exercise caution in imposing pre-existing statutory and regulatory classifications on Internet-based services"[383] because "such general frameworks may produce unintended results when applied to Internet-based services."[384] However, he also recognizes that the FCC will need to resolve some of these issues as the Internet continues to grow and new hybrid services develop.[385]

As a plan of action, he recommends that the FCC first identify areas "that clearly lie outside the scope of traditional regulatory requirements, so as to minimize market uncertainty while it confronts the more difficult categorization issues."[386] It should then:

> "identify relatively simple and flexible structures that achieve underlying policy goals. The initial assumption ought to be that new Internet-based services should not be subject to the regulatory constraints of traditional services. *Government policy should be sensitive to the fact that technology is changing rapidly, and that the Internet landscape a few years in the future may look very different than it does today.* [emphasis added] ... "The analytical process must work in both directions. Government should think not only about the regulatory treatment of new services, *but*

[381] Kevin Werbach, "Digital Tornado: The Internet and Telecommunications Policy," Federal Communications Commission Office of Plans and Policy Working Paper Series 29, March 1997, ii-iv.
[382] Werbach, "Digital Tornado," ii.
[383] *Ibid.* iv.
[384] *Ibid.* 33.
[385] *Ibid.* iv.
[386] *Ibid.* iv.

> *about the implications of those new services for the regulatory treatment of existing services.* [emphasis added] If a competitive imbalance exists because a new technology is not subject to the same regulatory constraints as a competing older technology, the answer should be reduced regulation of the older technology. Of course, such deregulation should be dependent on the existence of sufficient competition to police the actions of incumbents. The ultimate objective, however, should be less regulation for all, rather than more regulation for some."[387]

As discussed in the next section on FCC actions, the Commission did not entirely follow these recommendations with respect to VoIP. On one hand, it has largely functionally excluded IP-to-IP VoIP from traditional regulatory requirements. Some of the proceedings on VoIP, particularly in the comments, have shown sensitivity to the rapidly evolving nature of VoIP technology and the potential implications of that evolution on regulation. (e.g., the Stevens Report in 1998 notes that it is still early to decide how to characterize VoIP.) On the other hand, given that it has begun to impose those requirements on interconnected VoIP, and defined Class 1 VoIP as telecommunications, it has really created "more regulation for some" rather than "less regulation for all."

Werbach argues for sensitivity to changing technologies and the technological difficulties inherent in attempting to regulate them. With respect to VoIP in particular, Werbach notes that technical difficulties exist in the application of the current regulatory system. For example, in order to apply Title II of the Communications Act to Internet telephony, a system to determine which packets are telephony traffic and which are not must exist. Current Internet protocols do not allow for this type of monitoring, so a new system would need to be devised, which could be quite expensive. In addition, it would require defining what exactly constitutes an "Internet phone call," which is not obvious, and changing technology may render any "bright lines" obsolete very rapidly.[388] (45)

Werbach is deeply pessimistic and even cynical regarding the ability of regulators to make fine-grained regulations. He cautions against trying to "pick winners" rather than letting the marketplace decide, and encourages the FCC to instead focus on "eliminating regulatory roadblocks and other disincentives to investment."[389]

---

[387] *Ibid.* 47.
[388] *Ibid.* 45.
[389] *Ibid.* iv.

> "...No matter how sophisticated the regulator, companies in the marketplace will devise clever means of avoiding regulatory restrictions. No matter how well-intentioned the regulator, government intervention in the private sector can have unexpected and unfortunate consequences. Thus, government should apply blunt instruments that achieve underlying goals, rather than struggling for an elegant or precise solution that will cover every case. Wherever possible, market forces should be harnessed to take the place of direct regulatory intervention. Although new services like Internet telephony and streaming video may create legal headaches, these developments are positive ones that government should encourage. Such new technologies are valuable both because of the new options they represent for consumers, but also because of the potential competitive pressure they may exert on incumbent providers."[390]

The verdict on the FCC's success in achieving this goal is rather mixed when it comes to VoIP. Regulatory ambiguity continues to exist as regards VoIP, which is a disincentive to investment. The trend toward imposing more and more legacy regulations on interconnected VoIP, too, does not qualify as "eliminating regulatory roadblocks."

One portion of Werbach's paper that may have had a more positive influence on FCC action, however, is his argument against granting the America's Carriers Telecommunication Association (ACTA) petition of March 1996. ACTA, a trade association primarily comprised of small and medium-size interexchange carriers, sought a ruling from the Commission that VoIP providers were fundamentally analogous to switchless long-distance resellers, and should therefore be subject to the same access charge regime as LECs. Werbach argues that VoIP is fundamentally different from traditional telephony. The quality of service, ease of use, and technical requirements are all different. For example, while a circuit-switched call ties up an entire 56 kbps line for the duration of the call, with compression, a packet switched call can require only 4kbps while transmitting. Therefore, a cost comparison between the two is not obvious, so imposing access charges designed for traditional telephony on VoIP would be inappropriate.[391] Werbach's breakdown of the various misfits between the access charge regime and VoIP technology may have contributed to the FCC's eventual dismissal of the petition.

Oxman (1999)

Oxman's paper, which was published two years after Werbach's, was another passionate defense of the FCC's deregulatory approach toward the Internet. He argues that the FCC created a deregulatory environment that helped the Internet flourish, and that the FCC should continue

---

[390] *Ibid.* 46.
[391] *Ibid.* 38-40.

this policy.[392] Oxman points out that the regulatory and policy questions caused by the convergence of computers and communication have not been resolved since *Computer Inquiries* were launched to explore those issues. Rather, the Commission now faces difficulties fitting new technologies into old regulatory categories: "Where once data communications were offered "over" the voice network, the network of the future promises voice services as just another data offering. The FCC's challenge is to maintain its hands-off approach to the Internet in an era when traditionally regulated services, such as voice telephony, are offered over traditionally unregulated mechanisms, like the Internet Protocol. The Commission's instinct, as it has always been, should be to permit market forces to work, because competition leads to the widest variety of consumer choices."[393] While arguing that the Commission should "avoid regulation based solely on speculation of a potential future problem," he adds that the FCC should maintain oversight to "ensure that market forces do not fail or are otherwise unfairly manipulated by inappropriate behavior by entities with market power."[394]

Oxman concludes that the FCC should continue its deregulatory ("unregulation") approach to ensure that communications networks and Internet services dependent upon those networks continue to grow. He summarizes the lessons of the FCC's three decades of (de)regulating data networks:

- · Do not automatically impose legacy regulations on new technologies,
- · When Internet-based services replace traditional legacy services, begin to deregulate the old instead of regulate the new; and
- · Maintain a watchful eye to ensure that anticompetitive behavior does not develop, do not regulate based on the perception of potential future bottlenecks, and be careful that any regulatory responses are the minimum necessary and outweigh the costs of regulation.[395]

As with the Werbach paper, the FCC's adherence to Oxman's recommendations is mixed. The FCC's actions seem more consistent with a policy of not regulating than de-regulating. Certainly, with respect to the imposition of CALEA requirements, it has regulated somewhat in anticipation of problems: the FBI has been unable to produce evidence of VoIP technology

[392] Jason Oxman, "The FCC and the Unregulation of the Internet," Federal Communications Commission Office of Plans and Policy Working Paper Series 31, July 1999.
[393] *Ibid.* 25.
[394] *Ibid.* 25.
[395] *Ibid.* 3.

thwarting authorized wiretaps, even though this is a major justification for demanding the application of CALEA requirements to VoIP.[396] It has done somewhat better (?) resisting or delaying the demands of the various interest groups, at least on economic issues. For example, Oxman cites the U.S. West petition to declare that phone-to-phone VoIP providers are not enhanced service providers and should therefore be subject to the access charge regime.[397] The FCC took no action on the petition, and it was eventually withdrawn.

Pulver Order

The first FCC action toward formally defining or categorizing VoIP was the *Pulver Order*, issued in February 2004 in response to a Pulver.com petition.[398] Pulver.com had petitioned the Commission to declare its service not "telecommunications" or a "telecommunications service."[399] The Commission granted the petition. The Order stated that FWD was "neither telecommunications nor a telecommunications service" but an "unregulated information service."[400] It is noteworthy that the FCC rejected Pulver's interpretation of the definition of "information service." Pulver had argued that FWD was not an information service because it did not provide transmission capabilities.[401] The FCC overruled this reading, stating that information services need only *offer* computing capabilities *via* telecommunications.[402]

This was the first time the Commission had formally ruled whether a particular type of VoIP service was or was not telecommunications, meaning whether it would or would not be subject to the legacy telephony regulations. The Commission specifically noted that its decision was limited to the Pulver FWD service as it existed at the time of the petition: namely, without interconnection with the PSTN.[403]

---

[396] See Electronic Frontier Foundation (EFF), "Comments of the Electronic Frontier Foundation," and Electronic Privacy Information Center (EPIC), "Comments of the Privacy Information Center," Communications Assistance for Law Enforcement Act, RM-10865 (2004).

[397] See *Petition of U.S. WEST Inc. for Declaratory Ruling Affirming Carrier's Carrier Charges on IP Telephony* (filed April 5, 1999), in Oxman 22.

[398] *Pulver Order.*

[399] *Ibid.*

[400] *Ibid.*

[401] Ex parte Pulver letter of December 11, 2003, cited in *Pulver Order.*

[402] *Pulver Order*, ¶14.

[403] *Pulver Order,* footnote 3. "We reach our holdings in this Order based on FWD as described by Pulver in its petition and subsequent *ex partes*. We thus limit the determinations in this Order to Pulver's present FWD offering (only to the extent expressly described below), without regard to any possible future plans Pulver may have. *See, e.g.*, BellSouth Comments at 4 & n.13 (quoting a Pulver press statement about eventually charging a fee); USTA Reply at 4 (citing SBC Comments at 2 that FWD may eventually enable calls to users outside the FWD community).

As organizational theory would predict, the Commission took the opportunity to reassert its authority in such matters in the Order. The Order states: "We determine, consistent with our precedent regarding information services, that FWD is an unregulated information service and any state regulations that seek to treat FWD as a telecommunications service or otherwise subject it to public-utility type regulation would almost certainly pose a conflict with our policy of nonregulation."[404] The footnote restricts this assertion to the FWD service.[405] The Commission justifies its jurisdiction on two grounds. First, that "federal authority is preeminent in the area of information services... [even though] the Commission's traditional test for determining the boundaries of interstate versus intrastate jurisdiction – the end-to-end analysis – is inapplicable in the context of FWD and, even if it were applicable, would not support a finding of intrastate jurisdiction. Second, state-by-state regulation of a wholly Internet-based service is inconsistent with the controlling federal role over interstate commerce required by the Constitution.[406]

Vonage Order

In November 2004, the FCC repeated its assertion of authority over VoIP technologies in the *Vonage Order.* Vonage had petitioned the Commission for a declaratory ruling preempting an order of the Minnesota Public Utilities Commission that would impose traditional telephony regulations on Vonage's DigitalVoice VoIP service in September 2003. The Order states explicitly that the Commission was deliberately building up regulatory precedent for asserting its authority over VoIP:

> "We conclude that DigitalVoice cannot be separated into interstate and intrastate communications for compliance with Minnesota's requirements without negating valid federal policies and rules. In so doing, we add to the regulatory certainty we began building with other orders adopted this year regarding VoIP – the *Pulver Declaratory Ruling* and the *AT&T Declaratory Ruling* – by making clear that this Commission, not the state commissions, has the responsibility and obligation to

---

Furthermore, this declaratory ruling addresses FWD only to the extent it facilitates free communications over the Internet between one on-line FWD member using a broadband connection and other on-line FWD members using a broadband connection. Therefore, we specifically decline to extend our classification holdings to the legal status of FWD to the extent it is involved in any way in communications that originate or terminate on the public switched telephone network, or that may be made via dial-up access. *See* Letter from Susan M. Hafeli, Counsel, pulver.com, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 03-45, at 1 (filed Dec. 11, 2003) (Pulver Dec. 11 *Ex Parte* Letter) (acknowledging that "third parties can provide FWD subscribers with connectivity to the public switched telephone network" without Pulver's permission). Rather, we will address the legal status of those communications in our companion IP-Enabled Services rulemaking."

[404] *Pulver Order* ¶16

[405] *Pulver Order*, footnote 55.

[406] *Pulver Order* ¶16

> decide whether certain regulations apply to DigitalVoice and other IP-enabled services having the same capabilities. For such services, comparable regulations of other states must likewise yield to important federal objectives. Similarly, to the extent that other VoIP services are not the same as Vonage's but share similar basic characteristics, we believe it highly unlikely that the Commission would fail to preempt state regulation of those services to the same extent."[407]

It was classic bureaucratic turf-marking. By establishing this precedent, the Commission not only defended its organizational turf, as organizational theory suggests, it also protected VoIP from additional regulation. In other words, the preemption served the purposes of furthering the Commission's deregulatory agenda, by reserving the right to regulate to the Commission alone. It also allowed the Commission to ensure that the NPRM on IP-enabled services it had launched a few months prior would have minimal competition from state regulation. (See discussion of CALEA below)

Section 4. VoIP Issues and FCC Actions

The previous section discusses some of the legislation that governs regulation of VoIP and other telecommunications technologies. It also explains how VoIP does not fit neatly into the telecommunications service vs. enhanced services categorization system. The vast majority of these regulations apply only to telecommunications and telecommunications services, which is why the characterization of VoIP is so important.

In this section I discuss in further detail the regulatory obligations that characterization as a "telecommunications service" would bring on VoIP: disability access, universal service fund contributions, intercarrier compensation, emergency services (911/E911), and CALEA.[408] The first three (disability, USF, intercarrier compensation) are largely economic issues, and the latter two security (public safety, domestic security) issues. In this section, when I refer to uncertainties in applying regulation to VoIP, I am generally referring to Class 2 VoIP. Class 1 VoIP has already been defined as telecommunications, so there is no debate over whether it is subject to any of these requirements. It is. Class 3 VoIP, which the FCC has characterized as an information service in the *Pulver Order*, is not.

---

[407] *Vonage Order*

[408] Vaishnav, "VoIP," 93; Cybertelecom, "FCC," http://www.cybertelecom.org/voip/Fcc.htm (accessed January 24, 2008).

This section also discusses various actions the FCC has taken on VoIP with regards to these regulatory obligations. For the most part, comparatively little movement has occurred on the economic issues relative to the security issues. There has been very little attention paid to disability access due to the flexible nature of VoIP, which tends to accommodate disabilities more easily than traditional telephony. The access charge is the most economically significant issue with the highest stakes. Although most of the petitions on VoIP have been about this issue, very little decisive action has been taken. Of the three economic issues, the only one that has been settled to any degree is universal service. The FCC ruled in June 2006 that interconnected VoIP (VoIP connecting to the PSTN) would be subject to access charges. It is worth noting that USF and disability access are the obligations with the smallest economic impact (the smallest amount of money at stake). The big issues – intercarrier compensation and particularly access charges – are the ones with the greatest potential to impact industry structure and the bottom line of both incumbent telcos and the VoIP providers, since access charges in particular are what underlie the telecomm industry's financial structure.

Both of the security issues have been largely settled for interconnected VoIP. The FCC delayed imposing emergency service and CALEA obligations on VoIP until outside pressures, namely public and Congressional pressure for the former, and federal law enforcement for the latter, forced their hand.

Below is a summary table of issues and actions taken, reproduced from earlier in the chapter.

Issue	Current Obligation	VoIP Challenges	Actions Taken
Disability Access	• Ensure that service and equipment are "accessible to and usable by individuals with disabilities, if readily achievable • Do not install equipment, features, or functions that do not meet these requirements • Provide relay services	• standardization of communications modes • funding	• None
Universal Service	• Contribute funds • Rreceive funds	• Should VoIP pay into or receive funds from the USF?	• Interconnected VoIP must pay into USF
Intercarrier compensation	• Access charges • Reciprocal compensation • Other forms of compensation (voluntary)	• Arbitrage opportunities created by IP • Separation of signaling and content • Who pays? How much?	• None
911/E911	• Identify emergency calls and route to PSAP • Provide callback information • Provide location	• Different identifier • Devices are nomadic (E911 services depended upon customer to provide location) • Separation of access, transport and application	• Interconnected VoIP must provide capability for geographic location identifier and connection to nearest PSAP
CALEA	• Provide call-identifying information • Provide content tracing (lawful intercept) capabilities • Ensure security and privacy	• Call-identification information unknown to service provider • Tension between wiretap, security, privacy and innovation • Who pays?	• Interconnected VoIP must provide CALEA intercept capabilities • Carriers assume responsibility for costs

Figure 3.4 VoIP Regulatory Issues (repeat of Figure 3.2)[409]

Disability Access

Disability access requirements stem from the Americans with Disabilities Act of 1990 (ADA) and are reiterated in the 1996 Telecommunications Act with regards to

[409] Vaishnav, "VoIP," 88-93.

telecommunications providers (common carriers).[410] Disability access has not been a major issue in VoIP regulation. The technological flexibility of VoIP allows for multi-mode usage (text, voice, video) that actually provides easier compliance with disability access requirements than traditional telephony.[411] However, standardization of access requirements and funding remain to be resolved before manufacturers can easily provide disability access-compliant equipment.

To the best of my knowledge, the FCC has not taken any action with regards to applying disability access requirements to Class 2 VoIP. (Class 1 would automatically be subject to the requirements since it is defined as telecommunications service. In any case, since Class 1 VoIP is indistinguishable from traditional telephony to the user, presumably the service would already be disability access compliant.)

Universal Service Fund

The key questions in terms of USF and VoIP are whether VoIP providers are required to pay into the fund, and whether they are eligible to draw from the fund.

The rationale behind establishment of the Fund is pretty clear. The FCC writes that:

> "The goals of Universal Service, as mandated by the 1996 Act, are to promote the availability of quality services at just, reasonable, and affordable rates; increase access to advanced telecommunications services throughout the Nation; advance the availability of such services to all consumers, including those in low income, rural, insular, and high cost areas at rates that are reasonably comparable to those charged in urban areas. In addition, the 1996 Act states that all providers of telecommunications services should contribute to Federal universal service in some equitable and nondiscriminatory manner; there should be specific, predictable, and sufficient Federal and State mechanisms to preserve and advance universal service; all schools, classrooms, health care providers, and libraries should, generally, have access to advanced telecommunications services; and finally, that the Federal-State Joint Board and the Commission should determine those other principles that, consistent with the 1996 Act, are necessary to protect the public interest."[412]

There has been serious debate over the nature and appropriate uses of the USF.[413] While traditionally telephony has been largely based upon a system of cross-subsidies, with densely

---

[410] 42 U.S.C. § 12101, Public Law 101-336, 104 Stat. 327 (1990). The ADA defines a disability as "a physical or mental impairment that substantially limits a major life activity." 1996 Telecommunications Act, 47 U.S.C. §252.
[411] Vaishnav, "VoIP," 90.
[412] FCC, "Universal Service Homepage," http://www.fcc.gov/wcb/tapd/universal_service/ (accessed January 3, 2008).
[413] See Notice of Proposed Rulemaking (NPRM), Appropriate Framework for Broadband Access to the Internet over Wireline Facilities Universal Service Obligations of Broadband Providers, FCC 02-42, Docket No. 02-33 (February 15, 2002) ("Wireline Broadband NPRM"); Federal State Joint Board ("Joint Board") on Universal Service: Joint

populated urban areas and businesses paying higher rates in order to subsidize less densely populated (and therefore economically disadvantaged) rural areas, the interpretation and administration of this concept has some flexibility. The various stakeholders in the debate over USF seem to have identified their interests fairly quickly.

With specific application to VoIP, for example, Sen. Ted Stevens (R-Alaska) introduced a bill in January 2007 called the Universal Service for Americans Act (S.101) that would expand the universal service obligation to broadband ISPs and VoIP providers in order to fund broadband deployment in rural and low-income areas of the country. This was not the first time Sen. Stevens introduced versions of this bill; he had done so in the previous session of Congress as well.[414] Sen. John Sununu (R-NH) "argues that such subsidies distort competition and thwart progress in the arena of broadband access."[415] Meanwhile, a few Iowa-based companies have used USF subsidies to provide free international calling.[416] Perhaps unsurprisingly, both of these Senators are from states with a high proportion of residential customers and LECs that qualify for USF subsidies.

After considerable debate, the FCC ruled in June 2006 that all VoIP providers that connect to the PSTN must pay into the USF.[417] This decision was upheld in a challenge in the D.C. District court a year later.[418] In explaining the rationale behind the decision, FCC Chairman Kevin Martin stated that the obligation had been triggered by VoIP providers' own characterization of their services as "inherently interstate." He also justified the decision on the basis of "competitive neutrality", because allowing VoIP providers to not pay universal service obligations would favor VoIP technologies over other technologies.[419]

Board provides its recommendations concerning the process for designation of eligible telecommunications carriers and the Commission's rules regarding high-cost universal service support, Docket No. 96-45.

[414] "USA Act," 110th Cong., 1st sess., 2007, S. 101,

[415] "Universal Service Fund," http://en.wikipedia.org/wiki/Universal_service_fund (accessed August 8, 2007).

[416] Alex Saunders, "What's With the 712 Area Code?", Saunderslog.com, http://saunderslog.com/2006/10/11/whats-with-the-712-area-code/ (accessed August 8, 2007).

[417] Report and Order and Notice of Proposed Rulemaking, June 21, 2006, FCC 06-94, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-94A1.pdf; Anne Broache, "FCC Approves New Internet Phone Taxes", CNET News.com, June 21, 2006, http://news.com.com/FCC+approves+new+Internet+phone+taxes/2100-7352_3-6086437.html; Wayne Rash, "FCC Adds VoIP to Universal Service Fund," *Eweek.com*, at http://www.eweek.com/article2/0,1759,1980002,00.asp (all accessed January 31, 2008).

[418] Anne Broache, "Appeals court ruling upholds Net phone taxes", CNET News.com, June 1, 2007, http://news.com.com/Appeals+court+ruling+upholds+Net+phone+taxes/2100-7352_3-6188223.html?tag=item (accessed January 31, 2008).

[419] Statement of Chairman Kevin J. Martin, Re: Universal Service Contribution Methodology (WC Docket No. 06-122); Federal-State Joint Board on Universal Service (CC Docket No. 96-45); 1998 Biennial Regulatory Review –

Intercarrier Compensation

Intercarrier compensation is a high stakes game even without the added complication of VoIP. The current intercarrier compensation scheme derives from arrangements dating back to the AT&T divestiture and in the 1996 Telecommunications Act. The current flow of payments is estimated at around $14 billion a year.[420] Needless to say, this creates enormous incentives for telecom industry players to make sure they are getting their slice of the (very large) pie. The FCC has largely held off from any rulings on intercarrier compensation for Class 2 VoIP. This policy of inaction began with the 1998 Report to Congress on the Federal-State Joint Board on Universal Service ('Stevens Report').[421]

Intercarrier compensation is the term "used to describe arrangements governing who owes what to whom when two or more carriers cooperate to complete a call between subscribers to different networks."[422] It can take three forms: access charges and reciprocal compensation, which are tariffed at rates determined by the FCC, and voluntary negotiations, which are not. Access charges are generally fees paid by interexchange carriers (IXCs), or long distance carriers, to LECs for use of local loop facilities. Reciprocal compensation is generally paid between two LECs for terminating local calls on each others' networks. In general, reciprocal compensation rates are significantly lower than access charges. Access charge rates derive from the era of cross-subsidization, when long distance calls were assumed to be luxuries, and so long distance rates were set far above cost in order to subsidize local calls. This creates enormous arbitrage opportunities.[423] Voluntary negotiations are usually between a wireless carrier and LEC,

---

Streamlined Contributor Reporting Requirements Associated Administration of Telecommunications Relay Service, North American Numbering Local Number Portability, and Universal Service Support Mechanisms (CC Docket 98-171); Telecommunications Services for Individuals with Hearing and Speech Disabilities, and the Americans with Disabilities Act of 1990 (CC Docket No. 90- Administration of the North American Numbering Plan and North American Numbering Plan Cost Recovery Contribution Factor and Fund Size (CC Docket No.237; NSD File No. L-00-72); Number Resource Optimization (CC Docket No. 99-200), Telephone Number Portability (CC Docket No. 95-116); Truth-in-Billing and Billing Format (CC Docket No. 98-170); IP-Enabled Services (WC Docket No. 04-36), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266030A2.pdf

[420] Patrick Brogan, Intercarrier Compensation Reform (ICR) Framework for Gauging Investment Impact, Precursor Research (April 19, 2004), in Nuechterlein and Weiser, *Digital Crossroads*, 292.

[421] *Stevens Report.*

[422] Nuechterlein and Weiser, *Digital Crossroads*, 292.

[423] Two examples of arbitrage opportunities are the WorldCom scandal and the ISP reciprocal charge controversy. Both of these descriptions are drawn from Chapter 9 of Nuechterlein and Weiser.
The WorldCom/ MCI scandal was over WorldCom's alleged scheme to disguise long distance calls as local calls, thereby avoiding higher access charge fees and instead paying lower reciprocal compensation rates. WorldCom was a long-distance carrier. For example, imagine a WorldCom customer in Los Angeles called a Verizon customer in

determining rates paid to the LEC for use of the local loop. These rates are negotiated rather than set by the FCC.[424]

Intercarrier compensation exists because carriers must invest in switching and transport capacity to process all of the traffic that flows over their networks. However, the traffic flow may not be symmetrical. For example, imagine that most of the traffic between Nextel and BellSouth customers are calls placed *by* Nextel customers *to* BellSouth customers, because, for example, Nextel customers turn off their cell phones when not in use (or only use their phones to place

---

New York. Normally, WorldCom would incur an access charge fee for terminating the call on Verizon's New York network. However, if WorldCom were to instead send the call to a CLEC accomplice in New York, the CLEC could deliver the call to Verizon disguised as a local call, thereby only incurring the lower reciprocal compensation rate. WorldCom would be better off reimbursing the CLEC, and possibly paying a little extra on top of that fee, than paying the access charges.

The real question that the WorldCom issue raises is why there is such a large differential between access charges and reciprocal compensation rates. After all, the cost of completing the call for Verizon is the same whether it is handed off by WorldCom or the CLEC. It uses the same switch either way.

The second arbitrage example is ISP calls. Once the Internet became popular in the 1990s, many people used dialup connections over the PSTN to connect to the Internet. Users would call a local number, the modem of an Internet Service Provider (ISP) such as AOL or Earthlink, and the ISP would translate the analog signals from the call into digital signals and connect the user to various websites. These types of calls obviously feature asymmetric data flow. The FCC views these calls as long distance calls, even though technically the user is dialing a local number to the ISP. (Nuechterlein and Weiser reference generally *Bell Atl. Tel. Cos. V. FCC*, 206 F.3d 1, 5 (D.C. Cir. 2000)) Classifying such calls as long-distance is how the FCC justifies claiming jurisdiction over these calls and prevents states from regulating Internet access. However, if such calls are long distance calls, then they should be subject to per-minute access charges, like all other long distance calls. But the FCC has exempted such calls under the "ESP exemption." ISPs and other providers of enhanced services (now "information services," but the ESP exemption was put into place before the 1996 Act) are exempted from paying these access fees. Instead, they are treated as large institutional customers such as the banks and large companies that pay ILECs a flat monthly for use of business lines of comparable capacity. (Nuechterlein and Weiser reference Mem. Opinion and Order, *MTS and WATS Market Structure,* 97 FCC 2d 682, ¶¶ 76-83 (1983); NPRM, *Amendments of Part 69 of the Commission's Rules Relating to Enhanced Service Providers,* 2 FCC Rcd 4305, ¶ 2 (1987); NPRM, *IP-Enabled Services,* 19 FCC Rcd 4863 (2004)). The ESP exemption is usually what people are referring to when they talk about the FCC's decision not to regulate the Internet.

The arbitrage opportunity in the ISPs came when CLECs realized that the 'termination rate' for calls was set much higher than the actual cost of obtaining and maintaining a switch to serve an ISP modem bank. What CLECs do for the ISP is connect with the ILEC's network (the ILEC being the network serving the ISP subscribers, or the people trying to access the Internet), take the incoming call, route it through a switch that terminates the call on the ISP modem bank, and transport the call to the modem bank. In theory, the last two steps impose aggregate costs on the CLEC that the ILEC must compensate it for under the reciprocal compensation regime. In theory, if the rate set for terminating calls is equal to the actual cost of terminating the call, the ILEC pays the CLEC, and passes those costs on to its customers. (The poor guy who's still trying to get onto the Internet.) Unfortunately, the termination rates were set too high. This functionally meant the CLECs received a per-minutes subsidy for every call. Multiplied by huge call volume, CLECs realized that those subsidies became large enough that they could afford to not only charge ISPs nothing for servicing them, but *they actually competed over the privilege of serving ISPs – to the extent of even offering to pay ISPs outright for the privilege.* The ILECs, in turn, largely were unable to recoup the per-minute fees charged by the CLECs, because most residential customers paid flat-rate monthly fees for local service that were not usage-sensitive. Charging households with high call volume to ISPs was politically unpalatable to state commissions, too, since that would be seen as taxing the Internet. Neither was raising the flat monthly rate for everyone a politically tenable solution, since that would mean non-Internet users were subsidizing Internet users. (It would also violate the principle of providing cheap local service to all.)

[424] Vaishnav, "VoIP," 91-92; Nuechterlein and Weiser, *Digital Crossroads*, 292.

calls but do not answer incoming calls). This means that in order to fulfill its regulatory duty (as a telecommunications provider/ common carrier), BellSouth must on the margin purchase larger switches and transport pipes in order to carry more incoming telecommunications traffic. Nextel, on the other hand, does not need to invest in as much infrastructure to accommodate calls from BellSouth customers. Assuming that there is no contractual relationship between Nextel and BellSouth, who is responsible for the extra costs incurred by BellSouth to serve Nextel customers?[425]

One solution is called *bill-and-keep*. Under bill and keep, each carrier absorbs the extra costs on its own and passes them along to its subscribers by charging higher retail rates. The other solution shifts those costs onto the carrier that originates the call. This scheme is called *calling-party's-network-pays* (CPNP). CPNP has traditionally been the rule in the telecommunications industry.

The main questions VoIP raises for intercarrier compensation is whether VoIP providers should pay, at what rates, and whether those rates should be the same for all providers. Intercarrier compensation rates are wildly out of line with the actual costs of interconnection. Meanwhile, IP is agnostic with regards to the physical transport layer – packets do not care whether they are moved over cable, optical fiber, copper pairs, or airwaves (wireless). To further complicate matters, the underlying cost structure of each of these architectures is very different. Call signaling and content (bearer) channels can be separated in VoIP, so a facilities-based VoIP provider such as Comcast or Verizon that owns the physical facilities will have very different costs from non-facilities-based VoIP providers (Vonage, Skype). Should the rates be set at a uniform rate across providers, then? This creates arbitrage opportunities that can be exploited. owns the infrastructure will have a very different cost structure from the non-facilities-based VoIP provider (Skype).[426]

To date, it does not seem that the Commission has reached any conclusions on intercarrier compensation as applied to Class 2 VoIP. The Commission has exhibited a tendency to delay formalizing VoIP carrier's obligations with respect to the intercarrier compensation regime. In 1998, it deliberately held off from characterizing even Class 1 VoIP or ruling that it was subject to access charges, even though it noted that phone-to-phone VoIP seemed to "bear

[425] This and the following paragraph, including example, are drawn from Nuechterlein and Weiser, *Digital Crossroads*, 292.
[426] Vaishnav, "VoIP," 91.

the characteristics of "telecommunications services.""[427] "The FCC specifically declined to take any such action... indicating that to do so may stifle an emerging technology."[428] As the Stevens Report stated:

> "We defer a more definitive resolution of these issues pending the development of a more fully-developed record because we recognize the need, when dealing with emerging services and technologies in environments as dynamic as today's Internet and telecommunications markets, to have as complete information and input as possible."[429]

Instead, the FCC sought more time to allow the technologies to mature and to allow for more investigation into the various VoIP services offered.[430]

The tendency to delay decision-making continued in 1999, when U.S. West petitioned for a declaratory ruling that access charges apply to phone-to-phone IP telephony services provided over private IP networks. The Commission took no action on the petition, including putting the Petition out on Public Notice, and the petition was subsequently withdrawn when U.S. West merged with Qwest.[431] The motivation behind the delay in this case is less clear. The FCC did not give any reason for not acting on the petition, whether it be fear of aggravating various competing industry players or a desire to allow for more innovation in VoIP technology.

The U.S. West petition is one of the earliest instances of an ILEC identifying a VoIP service (Class 1) as a potential source of regulatory and competitive advantage, even though significant actual conflict had not yet arisen.[432] U.S. West stated that AT&T, Sprint, and other carriers were providing phone-to-phone telephony over their own private IP networks, but refusing to order access services to terminate and (in some cases) originate traffic. Instead, these carriers terminated traffic over local business lines or through CLECs that interconnected with the ILECs (such as U.S. West), so they would only have to pay reciprocal compensation rates rather than the much-higher access charge rates. U.S. West argued that the phone-to-phone IP

---

[427] Stevens Report ¶ 98.
[428] Chadbourne & Parke LLP, Client Alert: AT&T Seeks FCC Ruling Exempting IP Telephony from Access Charges, at http://www.chadbourne.com/files/Publication/4cdea554-a5b2-4d1b-9a15-82b6c468d525/Presentation/PublicationAttachment/95745a71-6def-42b0-80dd-8318534a9a71/AT&TSeeksFCCRulingExemptingIPTelephonyfromAccessCharges.pdf (accessed January 31, 2008).
[429] *Stevens Report* ¶ 90.
[430] *Stevens Report* ¶ 83.
[431] http://www.cybertelecom.org/voip/Fcc.htm
[432] Chadbourne, "AT&T."

services were "telecommunications services" under the 1996 Act and should therefore be required to use access services and pay access charges, as required by existing policy.[433]

Later, the Commission stated that "U.S. West nowhere attempted to square its request with the Universal Service Report's [Stevens Report, 1998] express holding that even if phone-to-phone IP telephony services were classified as telecom services, the Commission would have to address 'difficult and contested issues' before it could subject these services to access charges that are even 'similar' to those applicable to circuit switched interexchange services. The Commission did not issue a Public Notice of the US West petition or otherwise seek comment on it."[434]

In 2002, AT&T, one of the objects of the U.S. West petition, in turn filed a petition asking the Commission to declare its phone-to-phone IP telephony service exempt from access charges. AT&T argued that ILEC efforts to "to impose access charges on these services contravene the Congressional mandate to preserve the vibrant and free market that exists for the Internet, and the FCC's established policy of exempting [VoIP] traffic from access charges."[435] AT&T was referring to the 'ESP exemption', a long-standing FCC policy of exempting enhanced or information service providers such as ISPs from paying access charges. (ISPs instead paid the same flat monthly rates as comparably sized large institutional customers such as banks that were directly connected to CLEC networks.)

As with the U.S. West petition, it seems the AT&T petition was largely preemptive and precautionary, rather than a reaction to significant existing conflict. One legal analysis notes that "While it is true that there continue to be skirmishes between incumbent LECs and IXCs over the issues raised in the petition, it does not appear that there has been any particular proliferation in these disputes recently. In fact, the controversies cited by AT&T seem largely anecdotal, with incumbent LECs engaging in a bit of posturing, but ultimately provisioning the services that AT&T requests."[436]

In any case, the petition was denied on the basis that AT&T's service fulfilled all four criteria for a telecommunications service set out in the Stevens Report. The Stevens Report had

---

[433] From summary of U.S. West petition in *AT&T Order* ¶16. Petition at http://svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513386921 (accessed January 31, 2008).
[434] *AT&T Petition*
[435] *AT&T Petition*; Chadbourne, "AT&T".
[436] Chadbourne, "AT&T".

tentatively concluded that phone-to-phone IP telephony services were telecommunications because they met the following conditions:

> (1) it holds itself out as providing voice telephony or facsimile transmission service;
> (2) it does not require the customer to use CPE different from that CPE necessary to place an ordinary touch-tone call (or facsimile transmission) over the public switched telephone network;
> (3) it allows the customer to call telephone numbers assigned in accordance with the North American Numbering Plan, and associated international agreements; and
> (4) it transmits customer information without net change in form or content.[437]

Instead, the Commission ruled that AT&T's service was "telecommunications" and therefore subject to access charges.[438]

The formal denial of this petition in April 2004 was one of the first concrete actions the FCC took toward characterizing VoIP, with the exception of the tentative outlines set out in the Stevens Report. The vote itself was close, and controversial within the industry.[439] Given the Commission's history of delay or forbearance until then, it seems worth looking into what finally prompted action. (For example, the Stevens Report itself was only issued because of a clause inserted into an appropriations bill that required the FCC to produce that report.) It appears that the Commission was under some political pressure to make a ruling rather than drag its feet. According to *Phoneplusmag.com,* the Chairman of the House Committee on Energy and Commerce, which has jurisdiction over telecommunications, sent a letter to the FCC Chairman Michael Powell asking the agency to specify whether access charges applied to long distance VoIP.[440] Rep. Billy Tauzin (R-Louisiana) expressed the fears of the rural phone companies in his district that generated at least 60 percent of their operating revenues through access fees and USF support.[441]

---

[437] *Stevens Report* ¶ 88.
[438] *AT&T Petition*
[439] "FCC to Rule Against AT&T in VoIP Proceeding," *Telecom Policy Report,* April 21, 2004, http://findarticles.com/p/articles/mi_m0PJR/is_16_2/ai_n5994136 (accessed October 28, 2007).
[440] Josh Long, "FCC Under Pressure on VoIP: Congressman Demands Answers on AT&T Petition," *PhonePlusMag.com*, March 1, 2004, at *http://www.phoneplusmag.com/articles/431feat03.html*
[441] *Ibid.*

At the time of the ruling in 2004, there was still another three-year old proceeding on intercarrier compensation (CC Docket 01-92) pending. Meanwhile, another one had just been opened the same month (FCC 04-28, on "IP-Enabled Services".)[442]

In December 2003, Level 3 Communications filed a petition for forbearance, asking the FCC to exempt VoIP calls from access charges when terminating calls on the PSTN. Instead, the petition asks that VoIP providers be allowed to pay the lower reciprocal compensation rates. Level 3 argued in its petition that forbearance would allow IP-based telephony applications to flourish and innovation to continue.[443] However, Level 3 withdrew its petition a few days before the deadline for FCC action was set to expire. The reason cited was the change in leadership at the FCC the prior week, with the newly appointed Chairman Kevin Martin replacing outgoing Chairman Michael Powell.[444] It is not clear, however, whether the official reason behind the petition's withdrawal was true or whether Level 3 feared that the Commission might deny the petition, thereby codifying an adverse policy.

There are several possible explanations for the FCC's inaction with respect to intercarrier compensation and VoIP. First, the Commission could simply be exercising forbearance for purposes of encouraging innovation. Second, the Commission could have ulterior motives, hoping that VoIP would undermine the intercarrier compensation regime. Third, political deadlock among the Commissioners could explain inaction.

First, the Commission could be exercising forbearance for the purposes of encouraging VoIP innovation. As the Stevens Report noted (although more in conjunction with USF obligations), VoIP technologies had yet to mature and the Commission wished to encourage innovation. The 1996 Act charged the Commission with promoting competition and deregulation. There is also not only a deregulatory but an anti-regulatory streak in the Commission's ideology, as seen in the two OPP white papers. Werbach's argument against the ACTA petition's request to subject VoIP to access charges is particularly telling. Thus it is entirely possible that, although not explicitly stated, the Commission hoped that by not formalizing the access charge obligations on a VoIP provider, it would allow VoIP to grow into a viable competitor to traditional

---

[442] "FCC Rules on AT&T's VoIP Petition," http://www.techlawjournal.com/topstories/2004/20040421.asp (accessed September 20, 2007).
[443] David Sims, "VoIP to Pay PSTN Access Charges?" TMC Net.com, http://www.tmcnet.com/tmcnet/articles/2005/voip-pstn-charges-fcc-level3-forbearance.htm (accessed September 20, 2007)
[444] Grant Gross, "Level 3 withdraws VoIP petition before FCC," InfoWorld.com, March 22, 2005, at http://www.infoworld.com/article/05/03/22/HNlevelthreewithdraws_1.html (accessed September 20, 2007).

telephony. Since the objective of promoting competition is promoting consumer welfare through greater choice (and lower prices through competition), promoting VoIP development would be one way to satisfy the Commission's duty to promote deregulation and competition.

A second, more cynical interpretation involves the access charge regime. Allowing VoIP providers to undermine the access charge regime would be one way to force reform, whether through a complete overhaul of the system, a recalculation of rates (assuming they could be recalculated 'correctly'), or by other means. Most telecommunications experts believe the intercarrier compensation system is a hopelessly tangled and inefficient system. Moreover, it is a mess created and maintained by FCC policy, which for political reasons it cannot easily fix.[445]

The LECs that depend upon access charges for a majority of their income, particularly the smaller LECs, have very powerful allies in Congress. For example, at the time of the AT&T petition in 2002, the Chairman of the House Committee on Energy and Commerce came from a district with a constituency that includes many of these smaller, rural LECs. In the Senate, the ranking member and former Chairman of the Committee on Commerce, Science, and Transportation, which has jurisdiction over telecommunications, is Ted Stevens, senior Senator from Alaska, a state with many rural LECs. The current Chairman is Daniel Inouye of Hawaii, another state where geography is rather unfriendly to economies of scale in telecommunications. The larger ones LECs, even without the aid of their Congressmen, clearly have armies of lawyers able to slow down any attempt at reform perceived as detrimental to the LECs' bottom lines, as evidenced by the sheer mass of lawsuits on access charges winding their way through various state and federal courts.

Third, political stagnation between the five Commissioners at the FCC could explain the Commission's lack of action. The Commissioners are political actors: they are appointed by the President, confirmed by Congress, and chosen by political party affiliation in order to maintain a balance favoring the party in the White House. Add to the mix the enormous sums of money involved, the tendency for Commissioners to come from and go back into the telecommunications industry after their terms are over, and the long-standing history of the

---

[445] See, for example, Jonathan E. Neuchterlain and Philip J. Weiser, *Digital Crossroads,* 293-332; Robert Atkinson, "Internet Telephone Service: A New Era of Competition in Telecommunications," Policy Report, March 2005, Progressive Policy Institute, http://www.ndol.org/documents/VoIP.pdf (accessed January 26, 2008); Whitt, "Horizontal Leap."

telcos' cooperation with the FCC, and it produces a recipe for either regulatory capture or political deadlock.

Emergency Services (911 and E911)[446]

The Commission did not act on VoIP emergency services issues until May 2005, when Congressional and public pressure forced it to take quick action.

The current 911 emergency service system is required by law to provide three features:

- identification of emergency calls and routing to the appropriate public safety answering point (PSAP)
- callback information
- location information

The first requirement is associated with basic 911 service. The latter two requirements are additional services imposed by the Wireless Communications and Public Safety Act of 1999 as enhanced 911 (E911) features.[447] Routing to the appropriate PSAP is done by associating certain PSAPs with certain telephone exchanges. The mechanism for obtaining callback information and the physical address of the calling party's telephone number is a reverse telephone directly supplied by the telephone company.

VoIP throws a monkey wrench into all three of these procedures. First, a VoIP identifier is not a ten-digit telephone number, which is what the current 911 system is designed for. Second, the identifiers are specific to individuals, not locations, whereas the devices (and presumably the person making the emergency calls) are mobile. For example, a Vonage adapter from Boston (617 area code) can be plugged into any broadband connection in the US, so while it may appear that the call is coming from Boston, the caller could actually be located in Los Angeles, or even Europe or Asia. Third, the 911/E911 function on VoIP does not work if the power fails or if the

[446] With thanks to Chintan Vaishnav for laying out the problems in applying 911/E911 to VoIP.
[447] 47 U.S.C. 615a, http://en.wikipedia.org/wiki/Enhanced_911 (accessed January 31, 2008).

broadband connection fails, which is different from the PSTN system. VoIP-based emergency services are not as reliable.[448]

The FCC issued its first Report & Order (R&O) and Notice of Proposed Rulemaking (NPRM) on IP-Enabled Services and E911 Requirements for IP-Enabled Services on May 19, 2005. The Order required VoIP providers interconnecting with the PSTN to provide E911 emergency calling capabilities to their customers as a mandatory feature of the service.[449] The alacrity with which the FCC adopted this order may have had much to do with press coverage of incidents in which consumers using VoIP had been unable to access emergency services, with unfortunate consequences, which the Commission explicitly cited as a reason for its adoption of this order.[450] Given the relatively uncontroversial nature of the public safety issues at stake, it seems likely that the fact the FCC did not act on the issue until May 2005 was not due to deliberate forbearance or industry pressures, but simply a failure of the issue to come up until then. The "immediate" requirement for self-reporting that the Order imposes, too, is unusual.[451] Most FCC Orders grant affected parties several months or even more than a year to comply.

The Order applies only to interconnected VoIP service providers (connected to the PSTN). It does not apply to Class 3 VoIP service providers, including those that provide instant messaging or Internet gaming services, even those that contain a voice component.

The Order requires interconnected VoIP providers to deliver all 911 calls to the customer's local emergency operator as a standard part of service. It further requires the interconnected VoIP providers to "provide emergency operators with the call back number and location information of their customers (i.e., E911) where the emergency operator is capable of receiving it. Although the customer must provide the location information, the VoIP provider must provide the customer a means of updating this information, whether he or she is at home or

---

[448] For further discussion, see also Patrick Ryan, Tom Lookabaugh, and Douglas Sicker, "A Model for Emergency Service of VoIP Through Certification and Labeling," 58 *Federal Communications L.J. (2006)* 116, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=876052

[449] First Report and Order and Notice of Proposed Rulemaking, IP-Enabled Services, E911 Requirements for IP-Enabled Service Providers, 20 FCC Rcd. 10245, (May 19, 2005), http://www.fcc.gov/cgb/voip911order.pdf (accessed February 1, 2008). ("1st R&O and NPRM IP-Enabled Services")

[450] News Release, Commission Requires Interconnected VoIP Providers to Provide Enhanced 911 Service (May 19, 2005), http://fjallfoss.fcc.gov/edocs_public/openAttachment.do?link=DOC-258818A1.pdf (accessed October 20, 2007).

[451] First Report and Order and Notice of Proposed Rulemaking, FCC 05-116 (May 19, 2005), ¶1, http://www.fcc.gov/cgb/voip911order.pdf (accessed October 20, 2007)..

away from home." The Order also obligates interconnected VoIP providers to inform new and existing customers of the E911 capabilities and limitations of their service.

In order to facilitate interconnected VoIP providers' compliance with this Order, the Order requires incumbent LECs to "provide access to their E911 networks to any requesting telecommunications carrier. They must continue to provide access to trunks, selective routers, and E911 databases to competing carriers. The Commission will closely monitor this obligation.[452]

The Commission also stated its intention to adopt, in a future order, an advanced E911 solution that includes a method for determining the customer's location without the customer having to self report this information. In June 2007, it issued another NPRM on Wireless E911 Location Accuracy Requirements, Revision of the FCC's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems in response to a petition by the Association of Public-safety Communications Officials-International, Inc.[453]

CALEA

The regulatory issue the FCC has taken most extensive action on is CALEA. Although CALEA has existed since 1994, the Commission made no effort to apply CALEA requirements to VoIP until pressure from federal law enforcement agencies (LEAs) forced their hand in 2004. Although the Commission acknowledged the need to investigate CALEA applicability to VoIP in 1998, six years went by with no action. After the 2004 petition, however, the FCC moved uncharacteristically quickly on VoIP CALEA issues, issuing two separate NPRMs and two separate Reports & Orders in less than three years. These Orders granted almost all of the LEA's Joint Petition, largely ignoring the many concerns raised by various commenters.

The basic requirements of CALEA are that telecommunications providers must provide call identifying information, content tracing capabilities (lawful intercept, as with wiretaps), and ensure privacy and security. VoIP, for technological reasons, does not always easily accommodate such requirements, or at least not without serious consequences for security, privacy, and economic interests. For example, making VoIP applications that separate the call

---

[452] See News Release, Enhanced 911 Service.
[453] NPRM, 911 Requirements for IP-Enabled Service Providers, FCC 07-108, Docket Nos. 94-102, 05-196, 07-114, (June 1, 2007).

signaling and transport, such as Vonage, CALEA-compliant requires coordination between Vonage and Earthlink to synchronize recording with the origin and termination of the call. Other considerations, such as the impact of CALEA compliance on innovation and the security of the Internet, are discussed in Section 3.

Inaction

As far as I can tell, the first FCC action on CALEA implementation (for VoIP) was in October 1998. The Commission issued an NPRM on rules for fulfilling the technical requirements of CALEA, which included proposals on nine additional capabilities proposed by the FBI.[454] The NPRM noted that eventually there would need to be consideration of extending CALEA rules to "packet-mode" communications. This was the first harbinger of the CALEA-VoIP debate to come. However, full action – as in the opening of a docket on the issue – did not occur until 2004.

For the LEAs, the lack of action was probably due to relatively low usage of VoIP at that point in time. The inaction by the Commission may have two explanations. First, the Commission may simply have considered CALEA one of the regulatory obligations it did not yet want to impose on an emerging technology. Second, implementation of CALEA requirements over even traditional telephony had been held up for more than three years already due to a flurry of lawsuits. However, it was clear that all players (FCC, FBI, industry) were aware that it was an issue that would need to be dealt with in the future.

There is a marked contrast in the speed with which the FCC has subjected VoIP providers to the 'security' obligations of telecommunications services versus the economic ones. Under pressure from Congress and incumbent telcos, the FCC submitted a report to Congress in 1998, the "Stevens Report", which among other things noted that the Commission had not come to a conclusion regarding an appropriate legal or regulatory framework for IP telephony. Six years later, nothing had been decided for VoIP. By way of contrast, the FCC opened a docket on

[454] FNPRM, Communications Assistance for Law Enforcement Act, FCC 98-282, (October 22, 1998), http://www.askcalea.net/fcc/docs/fcc98282.pdf (accessed February 3, 2008).

(conventional telephony) CALEA in October 1997.[455] An Order and FNPRM followed a year later.[456] Three more Orders followed in 1999.[457]

A month after the *Pulver Order,* the FCC opened an NPRM on IP-Enabled Services (FCC 04-36).[458] It sought comment on how Internet based services could "continue to be subject to minimal regulation" but also still provide the "mechanisms to implement important social objectives, such as public safety, emergency 911, law enforcement access, consumer protections and disability access, [which] may change as communications migrate to Internet-enabled services.[459] CALEA was not mentioned.

Enter Law Enforcement—Action!

The six years of relative quiet on CALEA VoIP issues following the 1998 Stevens Report came to a crashing end in March 2004. (There had been plenty of activity with regards to CALEA's application to the PSTN.) The Commission received a Joint Petition from the DOJ, FBI, and Drug Enforcement Agency (DEA) demanding that the Commission "immediate resolution" of VoIP CALEA implementation issues.[460] Although the petition was highly controversial, the Commission included its demands almost in their entirety in the NRPM on CALEA and Broadband Access Services issued in August 2004.[461]

From this point on, political pressure from the LEAs would dominate Commission decision-making on VoIP CALEA issues. Up until this point, the FCC had dragged its feet with

---

[455] NPRM, Communications Assistance for Law Enforcement Act, FCC 97-356, Docket No. 97-213, (October 2, 1997), http://askcalea.net/fcc/docs/fcc97356.pdf (accessed February 3, 2008).

[456] Memorandum Opinion and Order, FCC 98-233 (September 10, 1998), http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc98223.pdf (accessed February 3, 2008); FNPRM, FCC 98-282, accessible at http://www.askcalea.net/fcc/1999.html

[457] FCC 99-11, to establish the system security and integrity regulations that telecommunications carriers must follow to comply with CALEA section 105; FCC 99-229, which clarifies which categories of service providers are subject to CALEA requirements; FCC 99-230, to adopt technical requirements for wireline, cellular, and broadband Personal Communications Services (PCS) carriers to comply with the assistance capability requirements prescribed by CALEA, all at accesssible at http://www.askcalea.net/fcc/1999.html

[458] NPRM, IP-Enabled Services, FCC 04-36, RM-10865, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-28A1.pdf (accessed January 31, 2008). ("*IP-Enabled Services NPRM.*")

[459] News Release, *IP-Enabled Services NPRM,* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243868A1.pdf (accessed January 31, 2008).

[460] Joint Petition for Expedited Rulemaking Concerning the Communications Assistance for Law Enforcement Act, FCC RM-10865, http://www.askcalea.net/pet/docs/20040310.calea.jper.pdf (accessed January 20, 2008). ("*Joint Petition*")

[461] NPRM, Communications Assistance for Law Enforcement Act and Broadband Access and Services, FCC 04-187, Docket No. 04-295 (August 4, 2004), http://www.techlawjournal.com/agencies/calea/20040809nprm.pdf (accessed January 20, 2008). ("*CALEA NPRM*")

regards to CALEA applicability to VoIP. However, faced with enormous pressure from law enforcement agencies, the FCC backed down. In the post-September 11 era, and with the Iraq War ramping up, the political atmosphere was not conducive toward any behavior hinting of weakness on security issues. The Joint Petition had very deliberately framed CALEA as providing "an invaluable and necessary tool for federal, state, and local law enforcement in their fight against *criminals, terrorists, and spies*. [emphasis added]"[462] The Commission gave in to the political pressure in the following years. Despite overwhelming negative comments from of the commenters except the law enforcement agencies, the Commission adopted almost all of the Joint Petition's provisions in the two R&O's issued in the next two years.

The Joint Petition was highly controversial. Based on the comments submitted, it seems the main points of contentions were (1) the definition of "telecommunications", which would determine which services and providers had to comply with CALEA; (2) requiring carriers to verify with the Commission before installing any equipment that they believed would not be subject to CALEA; (3) who had to pay for CALEA implementation costs, and how those would be funded; and (4) who would set compliance standards. The petition took a rather extreme position on CALEA issues, seeking the broadest possible interpretation of application. At least one of the comments noted that many of the demands were deliberately extreme, intended as a negotiating tactic, in contrast to the more conciliatory views that had been expressed in private meetings.[463] Nonetheless, the majority of the petition's proposals were eventually granted.

The breakdown of the comments on the NPRM is predictable. Perhaps unsurprisingly, every law enforcement agency and organization that submitted comments wholeheartedly supported the Joint Petition.[464] Reaction from civil liberties groups was uniformly negative, citing a variety of reasons to reject the petition. Industry reactions were more varied. VoIP

---

[462] *Joint Petition* ¶ 2.

[463] "We acknowledge that various press reports have indicated that the strident nature of this filing differs from a more conciliatory view that has been expressed in private meetings. In addition, public comments attributed to dedicated public servants such as Rich Thompson, supervisory special agent with the FBI, relating to .technology preclearance not expected by law enforcement serve to indicate that the strident tone of the petition is in part a negotiating tactic. Nonetheless, several issues remain that merit comment. If the Commission desires to maintain CALEA compliance for the rural areas of the country, it should be mindful that telecommunications is a capital-intensive business, subject to fundamental business tenets. The petitioning LEAs ignore the most basic of business practices. The Commission would be well served to put aside the petitioner's business model that fails to balance LEA desires with rural carrier cost issues." From Comments of the Concerned CALEA Compliant Carriers, In the Matter of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration, (2004). (Hereafter, "Comments of ____ on *Joint Petition.*")

[464] For example, see comments from National Narcotic Officers Association Coalition, National Sheriffs' Association, New York State Police, etc., on *Joint Petition.*

providers, ISPs, and small telephone companies were generally opposed, with most focusing on cost and standards issues. Larger corporations, such as AT&T and WorldCom/ MCI argued for allowing industry to set its own compliance standards. One rather amusingly self-serving comment came from Top Layer Networks, Inc., which enthusiastically supported the petition – and then pointed out that its own products were CALEA compliance solutions.[465]

The biggest point of dispute was over the definition of "telecommunications". CALEA obligations apply only to telecommunications providers. The problem is, CALEA and the 1996 Act use different definitions of "telecommunications." The Joint Petition chose to use a very broad interpretation of the CALEA definition, which was itself broader than the 1996 Act's definition. The petition stated that "broadband access services and broadband telephony services are subject to CALEA," with "broadband access services" and "broadband telephony services" defined so as to eliminate many of the excluding factors previously established by the Commission. For example, the petition argued that

- information services should not be automatically excluded
- telecommunications providers should include not only providers of transmission services but *also switching services,* including packet switching
- change in form or content should not be a criteria for determining whether something is a telecommunications service[466]

The definition adopted by the Joint Petition would include almost any form of broadband communications and providers, including cable, broadband ISPs, packet mode technologies, and almost every form of VoIP except peer-to-peer.

Many of the commenters objected to this interpretation of "telecommunications", as well as to the sweeping definition of "broadband access services" and "broadband telephony services." The statement that "CALEA does not categorically exclude providers of information services from the definition of "telecommunications carrier"" received particular attention from commenters, who viewed it as an unacceptable expansion of CALEA's scope.[467] For example, the Center for Democracy and Technology (CDT) wrote that CALEA specifically excludes the Internet and Internet services.

---

[465] Comments of Top Layer Networks, Inc., on *Joint Petition.*
[466] *Joint Petition*
[467] Comments of Center for Democracy and Technology on *Joint Petition.*

Several of the comments also noted that the LEAs, and particularly the FBI, were attempting to use the Commission to rewrite CALEA to re-insert provisions that had deliberately been removed by Congress during the legislative process.[468] Covad Communications pointedly states: "...in many respects, the Petitioners' proposals resemble rehashes of policy positions law enforcement previously took and lost in the Commission's previous CALEA implementation proceedings. Covad believes the Commission should not allow the Petitioners to resurrect old policy fights they have already lost in years past, under the guise of implementing rules for new broadband technologies."[469] The Internet Commerce Coalition argues that the petition is an expansion of both obligations and the parties subject to those obligations. It notes that the draft of the FBI's "Digital Telephony" proposal, which eventually became CALEA, applied only to "common carriers." A provision for application to "replacement network providers" was excluded because it was viewed as unnecessary. Now, the FBI in its Joint Petition "attempts to secure exactly what the FBI said it did not need in order to pursue the goals of CALEA network providers".[470] The American Association of Community Colleges, et. al. adds that when Congress passed CALEA in 1994, "Internet access was discussed at the time and was clearly exempted."[471] They further question whether it is within the jurisdiction of the Commission to decide this issue, arguing that "[i]f CALEA is to be amended as the Petition requests, it is the job of Congress, not the Commission, to do so."[472]

Another concern raised in the comments was over the impact on technological innovation that expanding the scope of CALEA would have. With one exception, all of the comments that raised the issue pointed to the chilling effects the petition's proposals would have. [473] For example, the ISP Internet Coalition writes that the Petition "seeks to overturn the balance struck by Congress between law enforcement and continued innovation. In essence, it asks to adopt a much broader version of CALEA – a version that Congress has already expressly rejected."[474]

---

[468] Comments of CDT, Covad Communications, Electronic Privacy Information Center (EPIC), ISP Internet Coalition, and Leap Wireless, on *Joint Petition.*
[469] Comments of Covad Communications 1. Covad's comments are particularly interesting because they were written by Jason Oxman, author of the OPP working paper discussed in the previous section.
[470] Comments of Internet Commerce Coalition on *Joint Petition.*
[471] Comments of American Ass'n of Community Colleges, et. al., on *Joint Petition.*
[472] *Ibid.*
[473] Comments of American Civil Liberties Union (ACLU), American Association of Community Colleges, Covad Communications, Global Crossing North America, Inc., Skype, US Telecommunications Association, VON Coalition, on *Joint Petition.*
[474] Comments of ISP Internet Coalition on *Joint Petition.*

Covad Communications express a similar sentiment, arguing that the proposals in the Petition "represent a vast overreach to institute unnecessary, burdensome new powers for law enforcement at the expense of innovation in the broadband space."[475] The American Association of Community Colleges points out that extending CALEA to Internet access would stifle innovation in universities, which is a primary source of Internet technology development, and therefore would inhibit innovation in Internet technology as a whole.[476]

The only exception to these overwhelmingly negative comments was in the Reply to Comments submitted by VeriSign. Their comments argued that it was not clear that imposing CALEA on VoIP would cause adverse effects on innovation. Instead, VeriSign pointed out that regulation could create new industries and sectors, too.

The FCC seems to have decided not to act on the Joint Petition's requiring "any carrier that believes that any of its current or planned equipment, facilities, or services are not subject to CALEA to immediately file a petition for clarification with the Commission to determine its CALEA obligations."[477] The implications of the statement would have genuinely stifling effects upon investment and innovation, since it required *pre-approval* of not only current but even *planned* equipment, facilities or services. This would essentially have put industry investment and innovation at the mercy of a government bureaucracy's review process. At best, the net effect would have been delay; at worst, a disincentive to invest or try anything new at all. The Cellular Telecommunications and Industry Association proposal cites the example of packet radio services as an example of a widely used technology that would not exist if similar regulation had been in place.[478] Their Comments further note that "Congress wanted to ensure that CALEA would not be an impediment to the development and deployment new technologies."[479] They cite a House Report stating that "[t]he Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies. The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies."[480]

---

[475] Comments of Covad Communications on *Joint Petition.*
[476] Comments of American Ass'n of Community Colleges, et al., on *Joint Petition.*
[477] *Joint Petition* 34.
[478] Comments of Cellular Telecommunications and Industry Association 22 on *Joint Petition.*
[479] *Ibid.* 23
[480] H.R. Rep. No. 103-827(I), reprinted in 1994 U.S.C.C.A.N., 3499.

The third issue, who would pay for CALEA compliance costs, was understandably a concern for industry.[481] The Joint Petition had demanded that the Commission rule that carriers were responsible for the costs of equipment, facilities, and services installed after January 1, 1995. This would include virtually *all* VoIP services and equipment, since VoIP had not been offered on any kind of industry-wide level up until that point. It would also include almost the entire infrastructure installed during the broadband rollout during the late 1990s and early 2000s. The Joint Petition also asked the Commission to rule that carriers could not include any of the CALEA implementation costs in their administrative charges to law enforcement, but should instead shift those costs onto their customers. This issue was important, because carriers were permitted to charge a per-intercept fee to law enforcement for implementing wiretaps.

Two pieces of legislation governed this question. CALEA had established a fund for compensating carriers for the costs of bringing equipment installed on and before January 1, 1995 into line with CALEA requirements, while carriers themselves were responsible for the costs of equipment installed afterward. The FBI/ DOJ administered this fund, which was almost fully drained by the time of the petition.[482] However, the Omnibus Crime Control and Safe Streets Act stated that the applicant for surveillance orders must compensate the carrier for "reasonable expenses incurred in providing such *facilities* or assistance. [emphasis added]"[483] Thus by some interpretations, these two pieces of legislations conflicted.

The Commission had previously ruled that "carriers can recover at least a portion of their CALEA software and hardware costs by charging [Law Enforcement], for each electronic surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of the specific costs associated with each order."[484] In their Comments, Leap Wireless argued that "the statute does not preclude carriers from recovering capital costs and specific variable costs from Law Enforcement that are associated with individual intercept requests. These costs are "reasonable expenses incurred in providing . . . facilities and assistance" to be reimbursed by Law Enforcement under various federal and state surveillance statutes.[485] Leap gave a detailed breakdown of costs associated with implementing wiretap orders, including

---

[481] Comments from SBC, BellSouth, Leap Wireless on *Joint Petition.*
[482] Comments of the United States Telecom Association on *Joint Petition.*
[483] 18 U.S.C. § 2518
[484] *Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896, ¶ 60 (2002) (citing 47 U.S.C. § 229(e) "and collateral state regulations"), quoted in Comments of Leap Wireless on *Joint Petition.* 9.
[485] Comments of Leap Wireless, 8-9.

capital costs (equipment), staffing, and recurring costs (software upgrades), noting that the per-wiretap compensation rates charged covered barely half of the actual costs.[486] The Cellular Telecommunications and Industry Association also point out that the original rationale behind the Commission's approval of the FBI 'punch list' (the list of requirements to make equipment and facilities CALEA compliant) was based on the assumption that carriers could recover a portion of those costs from law enforcement. Reversing that source of funding in response to the Petition, when the window for appealing the prior decision had already passed, would be therefore unreasonable.[487] Several of the comments also noted that the high capital costs associated with CALEA compliance would be extremely burdensome to small, rural carriers.[488]

The fourth controversial issue was the Joint Petition's request that the Commission set the technical requirements or standards for compliance with CALEA. The text of CALEA had granted the Commission that authority *if* industry standard-setting organizations failed to issue technical standards or if industry-adopted standards were deficient.[489] Almost uniformly, comments from carriers argued that industry should be allowed to continue setting their standards, rather than having them imposed by the Commission. Law enforcement, on the other hand, argued that voluntary industry compliance had not and would not work.[490]

The Commission acted relatively quickly on the CALEA NPRM. It also granted almost all of the Joint Petition's requests that made it into the NPRM. (Since the issue of pre-installation review of equipment and services potentially not subject to CALEA had not made it into the NPRM, it was not considered in the Orders.)

The Commission issued its first Report and Order and a FNPRM less than a year later, on August 2005.[491] For the most part, the Order was a victory for the LEAs. The Order stated that "facilities-based broadband and interconnected VoIP", VoIP that connects to the PSTN, must be CALEA compliant. It also accepted that the CALEA definition of "telecommunications carrier"

---

[486] *Ibid.* 6-7.
[487] Comments of Cellular Telecommunications and Industry Association, 24-26.
[488] Concerned CALEA Compliant Carriers, Rural Iowa Independent Telephone Association
[489] 47 U.S.C. § 1006(b)
[490] See generally, Comments of Los Angeles Country Regional Criminal Information Clearinghouse
[491] First Report and Order and FNPRM, Communications Assistance for law Enforcement Act and Broadband Access and Services, FCC 05-153, ET Docket No. 04-295, RM-10865, (August 5, 2005), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf (accessed January 31, 2008). ("*1st R&O IP-Enabled Services*").

is "broader and can include services that are not classified as telecommunications services under the Communications Act."[492] The Commission agreed with the Joint Petition, deciding that facilities-based broadband and interconnected VoIP constituted a replacement for conventional telecommunications services and could therefore be deemed "telecommunications carriers," thereby making them subject to CALEA.[493]

However, even though the Commission faced enormous pressure from law enforcement to define VoIP for CALEA purposes, it still has not done so for the telecommunications industry as a whole. That is to say, the Commission ruled that IP-to-PSTN VoIP was a telecommunications service *under CALEA definitions, not for the wider regulatory sphere.*

The First R&O also adopted a FNPRM seeking more information on "whether certain classes or categories of facilities-based broadband Internet access providers – notably small and rural providers and providers of broadband networks for educational and research institutions – should be exempt from CALEA." That question took less than six months to answer in the Second R&O issued in May 2006.[494] The Second R&O reaffirmed compliance deadlines, which have often been largely ineffective (due to widespread use of petitions for extensions), for facilities-based broadband Internet access and interconnected VoIP services.

The LEAs also won on the cost issue, with the Second R&O concluding that "carriers are responsible for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities, and declines to adopt a national surcharge to recover CALEA costs. The *Order* finds that it would not serve the public interest to implement a national surcharge because such a mechanism would increase the administrative burden placed upon the carriers and provide little incentive for them to minimize their costs."[495]

The one issue it seems that the LEAs did not get their way on was the question of who would set CALEA compliance standards. The Commission affirmed in the Second R&O that "it would be premature to intervene in the process of developing assistance capability standards, as no petitions have been filed arguing that the current (ongoing) process being undertaken by telecommunications standards-setting bodies, acting in concert with LEAs and other interested

---

[492] News Release for *1st R&O IP-Enabled Services*
[493] *Ibid.*
[494] Second Report and Order and Memorandum and Opinion and Order, Communications Assistance for law Enforcement Act and Broadband Access and Services, FCC 06-56, ET Docket No. 04-295, RM-10865, (May 3, 2006), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (accessed January 31, 2008). ("*2nd R&O IP-Enabled Services.*")
[495] *Ibid.*

parties, is deficient." It also allows telecommunications carriers to use Third Parties (TTPs) to help them meet CALEA obligations, such as providing electronic surveillance information in the appropriate format. However, the Order notes, the carrier still retains ultimate responsibility "for ensuring the timely delivery of call-identifying information and call content information to a LEA and for protecting subscriber privacy, as required by CALEA."

Overall, it seems that the Commission's policy of refraining from imposing arduous regulation upon VoIP dissolved when faced with immense political pressure from law enforcement agencies brandishing national and domestic security as their justification for regulation. The speed with which the usually slow-moving Commission acted, and the fact the Commission granted almost all of the LEA's demands, suggests that national security arguments may continue to be one of the most effective spurs to action for the Commission.

Conclusion

This chapter has attempted to draw out how for nearly a decade the FCC refrained from imposing regulation on VoIP in order to allow VoIP technology to mature and innovation to continue. For the most part, the Commission was successful in holding off demands to impose an assortment of legacy regulations originally designed for traditional telephony until around 2004.

One major mechanism that the Commission utilized in its wait-and-let-develop strategy was its refusal to formally characterize VoIP as either a telecommunications service or information service. Characterization as the former would have automatically triggered legacy regulation, which the Commission feared would stifle innovation. Characterization as the latter, while freeing the technology from regulation, would also have limited the Commission's options in the future, since it was unsure how VoIP would evolve. Thus, the Commission charted a course that preserved its options for the future while attempting also to preserve some 'breathing room' for an emerging technology.

In refraining from regulating a sector it clearly had jurisdiction over, the Commission acted contrary to how conventional political science theory would expect a regulatory agency to behave. The one behavior exhibited by the Commission that fits well with the behavior predicted by organizational theory is its assertion of jurisdiction over VoIP—that is, protecting (or claiming, depending on one's legal interpretation) its bureaucratic turf. I argued here that the Commission's long history of dealing with emerging technologies had taught it that it was

always easier to regulate in the future than to undo previously imposed regulations, which would acquire constituencies that would fight change. The Commission's history had shown that regulating too early, or worse, ineffectively, could create so much uncertainty as to drive investment from a particular sector. This knowledge, combined with the deregulatory, pro-competitive mission that the 1996 Telecommunications Act had charged it with, led it to avoid regulating VoIP until external circumstances forced the Commission's hand.

By 2004, pressure from Congress and law enforcement pushed the Commission into action on universal service and CALEA. The contrast between the Commission's prior history of inaction and the speed with which it gave in to most of the law enforcement agencies' demands is quite noteworthy. Congressional and public pressure also forced movement on the 911/E911 public safety issue. Thus of the five issues outlined in this chapter, the only one that remains unresolved is intercarrier compensation, arguably the most complex and convoluted – and highest stakes – issue. The intercarrier compensation issue, it seems, is largely being decided in the courts.

This page intentionally left blank.

Chapter 4

Similarities and Differences between the Cases

Introduction

The NSA and FCC showed foresight in their management of commercial encryption and VoIP. Despite the conventional view of organizations as being reactive in response to new technologies, both organizations exhibited a willingness to anticipate the changes that each respective technology would bring and to proactively develop policies to manage those changes and protect their organizational interests. The central role that technology played in each organization's mission created an incentive to not only be aware of but to anticipate these changes. That is, unlike most organizations adapting to new technologies, the emerging technologies in question were not a means to an end, but the ends themselves: creating and breaking cryptographic codes is at the core of the NSA's mission, and regulating telecommunications technologies is the FCC's function. For the NSA, the threat that commercial cryptography posed to their core mission may also have created the impetus that allowed them to overcome barriers within their organizational culture.[496]

Both the NSA and FCC adopted policies that allowed for adaptation as the technologies matured and uncertainties resolved themselves. Their similar approach stemmed from their prior experience in managing and working with new technologies, which had impressed upon them the need to build flexibility into their policies to accommodate the uncertainties that accompany emerging technologies. Both organizations understood their respective technologies on a technical level. More unusually, they also seemed conscious of the limits to their knowledge. They seemed to recognize there were not only technological uncertainties, but also political, economic, and to a lesser extent, social uncertainties. If anything, technological uncertainty, even against a background of a rapidly changing technological environment that spanned the PC revolution and the introduction of the Internet, seemed of less significance than the uncertainties produced by new economic actors and political changes. This was particularly true for the NSA.

---

[496] An additional explanation for both organizations' ability to exercise foresight and execute forward-looking policies may lie within the organizational structures or with personality characteristics of the organizations' leaders. There is an extensive literature, particularly in the business school literature, that explores how individual leaders and organizational structures can and cannot foster innovation, and to a lesser extent, foresight. Regrettably, I was not able to fully explore these explanations in this dissertation. I was more interested in technology regulation and management, which is not a function of the businesses that this literature focuses on.

The NSA may have believed that it understood where commercial encryption was going on a technological level. However, it was less able to accurately foresee how the economic and political landscape would develop as the software industry grew in economic and political importance, and the end of the Cold War reduced the perceived national security threats motivating much of the NSA's mission. The FCC faced technological uncertainty with respect to how VoIP would develop. The Commission's greater concern, though, was how VoIP would impact the economic landscape, and specifically how VoIP would affect existing players who might try to stifle VoIP to prevent competition. The FCC also had to contend with a regulatory and legal framework, written for an older technology (telephones), into which VoIP did not readily fit.

Recognition of uncertainty and the need for flexibility did not limit the two organizations to the same policy. The NSA and FCC adopted two very different approaches to the management of encryption and VoIP. The NSA's strategy of slowing down and weakening the development and widespread use of commercial encryption led it to actively manage the technology. It influenced the technical development of commercial encryption through the export control process, intervened in the federal standards setting processes, attempted to limit access to and dissemination of cryptographic knowledge, and even recruited bureaucratic allies to propose legislation to mandate preferred policies. The FCC, by way of contrast, favored a policy of forbearance. It deliberately refrained from regulating VoIP in order to allow the technology to mature. Until forced to take action due to pressure from outside interests such as law enforcement, the Commission repeatedly denied petitions to regulate VoIP and asserted jurisdiction over VoIP in order to protect it from state regulation.

The contrast in their approaches to technology management seems to be due in large part to the different functional roles of each agency as well as their own confidence in their knowledge of the technology.[497] The NSA took a far more hands-on approach to managing commercial encryption than did the FCC with VoIP. During the 1970s and 1980s, the NSA's approach could be characterized as micromanagement. It is possible that this is because the NSA perceived itself as facing less technological uncertainty than did the FCC due to a combination of

[497] The NSA is an operating agency while the FCC is a regulatory agency. Undoubtedly, this difference played a role in the agencies' differing approaches to technology management. As noted in the Introduction, the cases are not wholly comparable, and this is the primary way in which they are not. I attempt to account for this as much as possible in the analysis, but as I note later in the chapter and in the Conclusion, ideally further research would attempt to tease out how much and in what ways this variable matters.

technological superiority vis-à-vis commercial cryptography and the lead time in previewing new cryptographic developments that the export control review process granted the NSA. The NSA also had an obvious interest in suppressing the technology, which the FCC lacked. The greater technological uncertainty, coupled with the more difficult task of promoting rather than discouraging technological innovation, may well account for the FCC's more cautious policy of forbearance.

Roadmap

The rest of this chapter is divided into three sections. The first section discusses the ways in which the foresight the NSA and FCC showed was unusual. The second discusses possible reasons that each organization was able to look forward and formulate effective policies to manage their respective emerging technologies. The third section discusses differences between the NSA and FCC's policies toward managing encryption and VoIP and possible reasons for those differences. The fourth section looks at the unanswered questions this study raises and possible alternative explanations.

Section 1. Foresight is Unusual

The foresight each organization showed runs counter to the conventional view of organizations as un-self-reflective, inflexible, and reactive.[498] First, it required both organizations to look forward and formulate a policy for dealing with the emerging technology before it had even begun to affect them. Organizational and bureaucratic theories both suggest that organizations favor routine, and do not act outside of those routines except when forced, as in times of crisis. (Some variants of bureaucratic theory suggest that even crisis may not be enough to force bureaucracies out of standard operating procedure, but instead causes them to cling even more tightly to routine.)[499] Second, both organizations were quite sensitive to uncertainty. Rather than relying solely on their technical expertise and assuming a linear extrapolation to predict the future, both organizations seemed to recognize that other types of uncertainty, not limited to technological uncertainty, would play a major role in shaping the

[498] See "Reactive vs. Proactive Change," http://www.referenceforbusiness.com/management/Pr-Sa/Reactive-vs-Proactive-Change.html (accessed January 6, 2008) for a summary of various articles in the business literature on reactive versus proactive change.

[499] Depending on how one reads the models, both variants can be found in Allison, "Conceptual Models.".

future. Third, as a result, both the NSA and FCC were able to recognize the need for flexible policies that could adapt to accommodate changes as the technologies developed and uncertainties resolved themselves. If anything, in adopting their policies, both organizations also consciously helped shape that future and how the uncertainties unfolded. Fourth, in the case of the NSA, the organization showed remarkable tactical adaptability in the execution of its strategy, even to the extent of acting contrary to an organizational culture of secrecy. This adaptability was not as apparent in the FCC case, partly because the policy of forbearance limited action, and partly because the FCC's existing bureaucratic delay tactics were quite effective.

Looking forward

The willingness of both the NSA and FCC to proactively examine the potential impact of their respective emerging technologies and act was rather unusual. Organizational and bureaucratic theories state that organizations are reactive. While many organizations do strategic planning and long-term studies, and even have specialized personnel or groups devoted to this purpose, often these reports are doomed to become shelfware.[500] Alternatively, factions within the organizations view them as suspect, written justification for existing policies or policies favored by another faction. Rarely are the results of internal studies implemented, much less effectively.[501]

The FCC seems to have unusually thoughtful in this regard. It not only looked forward, it did so with an eye to the lessons of history. Note that it is the lessons, or common principles, that I refer to here. The FCC did not assume incremental change, make a linear projection based on existing conditions, and call it foresight. In both of the Office of Plans and Policy working papers discussed in Chapter 3, the authors note how the FCC's past policy of encouraging Internet technologies through a hands-off policy had fostered innovation, and argued for a continuation of that policy. Werbach in particular warned of the hazards of too-early regulation and its stifling impact upon innovation.

---

[500] Thanks to Alexa McCray for reminding me about "shelfware" and routine, and routinely ignored, strategic studies. From personal experience producing such shelfware for the Office of Net Assessment in the Department of Defense, the fact that most studies are ignored seems entirely plausible.

[501] Aaron Wildavsky, "The Self-Evaluating Organization," *Public Administration Review* 32:5 (Sept.-Oct. 1972): 509-520; Stephen van Evera, "Why States Believe Foolish Ideas: Non-Self-Evaluation by States and Societies," unpublished paper, Department of Political Science, Massachusetts Institute of Technology. Clearly, a failure to self-evaluate or to implement the results of a self-evaluation is not the same as a failure to exhibit foresight. However, it does demonstrate that most organizations do not manage to effect change in the absence of crisis well.

Prior experience with other emerging technologies had shown that poorly written regulation could deter entrants into the market and slow technological innovation, as occurred with *Computer I.* Despite the years that went into its writing, the guidelines that *Computer I* established for determining what was and was not data processing were so confusing that they actually deterred entry into the data processing market. Companies did not want to enter the market for fear that a product they intended to fall into the data-processing (unregulated) category might instead be classified as regulated.

The FCC was also aware that regulation could create constituencies that would later hinder or prevent changes in regulation. This was undoubtedly a lesson from its decades of experience in working with various politically powerful monopoly industries, such as the cable companies, telephone companies, and radio/ media conglomerates. As such, the FCC tried not to regulate before the technology was mature in order to avoid creating entrenched interests.

The NSA also seems to have anticipated that trends in commercial technology worked against its interests, and that they would be unable to stop them. Bureaucratic theory suggests that in such a situation organizations may fall into standard operating procedure, either denying what is happening or pursuing existing actions more intensely in hopes of reversing the tide. The NSA, however, accepted the inevitability of change and instead found a way to limit its impact on its organizational interests proactively, long before mass market encryption had become a reality. Beginning with its involvement in the setting of technical specifications for DES, and later echoed in the approval process for the ciphers used in Lotus Notes and versions of Microsoft Windows, the NSA used bureaucratic processes to both gain access to and hinder the release of what it considered unacceptably strong encryption. Its later attempts to replace DES with a more NSA-friendly encryption standard (CCEP), and the initiative it took in submitting a Digital Signature Standard, were also future-oriented actions. Its most interesting behavior in terms of positioning itself for the future, however, was its recruitment of the FBI and other law enforcement agencies as bureaucratic allies to push the limited-encryption agenda, in the form of Digital Telephony (later CALEA) and the Clipper Chip, to Congress, the incoming Clinton administration, and (far less successfully) the American public. What makes these actions especially remarkable is that they required the NSA to act against its long-established organizational culture of secrecy and isolation and engage with not only other government agencies but even the American public—and that the NSA was willing to do it.

Put simply, the NSA and FCC each showed a willingness to look forward, and a willingness to act upon the conclusions of that look forward, that the conventional view of organizations would not expect.

Recognition of Uncertainty

Foresight as practiced by organizations often consists of simply extending the past into the future in a linear fashion. This can predict relatively minor or incremental changes, but not revolutionary ones such as those the NSA and FCC both faced at the end of the Cold War: the PC revolution, Internet, and broadband revolution. What both organizations, and the NSA in particular, did was to interpret trends in technological and economic changes and find policies that could achieve their goals only knowing the general direction technology was headed.[502] To use a sailing analogy, they found the direction of the wind and came up with a way to harness it to get where they were going, without knowing the exact speed or when each gust would hit. In the case of the NSA, even though the winds were blowing against it, the Agency found a way to tack against the wind so that they could still achieve their goals.

Although the NSA never explicitly stated its policy nor its characterization of the various uncertainties it faced, it seems apparent from their actions that they recognized that trends in technology, politics, economics and even society all pushed against their interests. The adeptness with which they sought to turn the uncertainties in each of those sectors to their advantage suggests that they recognized the uncertainties and had put some thought into how to counter them. The growth in commercial, mass market encryption was unstoppable—but still slowable. The precise form the encryption technologies would take, whether as code or chips, strong or weak algorithms, short or long keys, built-in or not, universal or with international and domestic versions, however, were up for grabs, and it was these uncertainties that the NSA tried to exploit through the export control review process and through legislation (CALEA, Clipper Chip). The Agency probably also recognized that with détente, and especially the end of the Cold War, the national security imperative that had allowed them relative freedom of operation – regulatory capture of Congressional committees, freedom from domestic intelligence laws, etc. – was breaking down. This meant that the entire political environment in which they operated would

[502] For this characterization of foresight, see Mike McMaster, "Foresight: Exploring the Structure of the Future," *Long Range Planning*, 29:2 (1996): 149-55.

change. Clearly, some sort of strategy or policy response was required that could accommodate those changes, which will be discussed in the next section.

The FCC was quite upfront about stating that its reservations in categorizing VoIP were due to the various technological, economic and political (regulatory) uncertainties surrounding the still-immature technology. In the Stevens Report in 1998, the Commission stated quite simply that had not yet determined an appropriate legal and regulatory framework for VoIP, a position it repeated in a series of forums and statements up through almost 2004. Implicit, and sometimes explicit, in these statements was the recognition that existing industry players held significant economic stakes in the FCC's decision, and that both existing and not-yet-existing players could significantly alter the VoIP technologies and how and whether they ever became viable.

Perhaps unusually for a regulatory agency, the Commission seemed aware of the limits of its own ability to predict the effects of its own regulation—and in particular of the "unexpected and unfortunate consequences" of even the most "well-intentioned" regulations.[503] In Werbach's paper, which was quite influential within the FCC, he encouraged the promotion of new technologies such as VoIP because they would create competitive pressure on incumbent service providers even as he acknowledged the "legal headaches" the new technologies created.[504] He did so knowing that VoIP and similarly revolutionary technologies could fundamentally alter the composition and nature of the telecommunications (telephone) industry. This is particularly true with regard to how VoIP could undermine the intercarrier compensation regime, which some telecommunications industry observers believe the FCC would like to change but cannot due to entrenched interests' resistance.

Overall, the recognition of the many forms that uncertainty took, not just limited to technological uncertainty, played a central role in determining both the NSA and FCC's responses to encryption and VoIP. Neither organization attempted to predict the future in any concrete way, but instead tried to maximize its own interests and ability to execute its mission under the constraints of a changing environment. This leads to the following point, the flexibility

---

[503] Werbach, "Digital Tornado," 46.

[504] I say that the paper was quite influential based on a telephone interview with Robert Pepper, the former head of the Office of Plans and Policy, who directed me to Werbach's paper as being one of the best and most widely read on the topic of VoIP regulation. (Robert Pepper, telephone interview, October 12, 2006).

of the policies each organization adopted in order to accommodate the changes they knew would occur.

Flexible policy

The flexibility of the policies that both the NSA and FCC adopted seems unusual among government agencies for their being able to take into account not only change, but the direction of change. Adaptation and flexibility are often cited as desirable traits that various government agencies try to achieve, but actually doing so while following a consistent strategy that is not so vague as to be useless seems rarer. (The danger lies in an organization that adopts a 'strategy' so flexible that it is functionally indistinguishable from having no strategy at all, and instead is purely responsive.) The NSA's strategy of reducing and slowing down mass market encryption, and the early recognition of the inevitability of its spread, was actually an unusually subtle strategy that probably worked better for its appearing so ham-handed on the surface. The FCC's policy of forbearance was perhaps even more unusual, strategically if not tactically. Forbearance seems to be quite rare among government agencies, although the stalling tactics and bureaucratic turf-claiming the FCC used to execute the strategy are common enough.[505] In both cases, the NSA and FCC did not simply say that they would accommodate change, they did so having an idea of the general direction and form those changes would take.

The FCC repeatedly stated that it believed that Internet-based technologies would be a key driver of technological change in the future, and that the FCC's policy of not regulating the Internet and allowing market forces to work had been a key factor in its growth.[506] This belief formed the basis for the policy of forbearance with respect to regulating VoIP—the principle of "avoid regulation based on speculation of future problems."[507] However, the FCC also

---

[505] Without doing a multiple cross-case comparison of government agencies, I cannot state decisively that forbearance is unusual among government agencies. However, from an e-mail communication with Jeff Lubbers, an expert in regulatory procedure and administrative law, and from multiple conversations with Larry McCray, the founding director of the Policy Division of the National Research Council of the National Academy of Sciences, it seems that forbearance is relatively unusual. Neither could think of another example of regulatory forbearance. Lubbers and McCray have both suggested that the best way to approach this question might be to look at other agencies that frequently deal with emerging technologies, such as the Food and Drug Administration (FDA), Environmental Protection Agency (EPA), and Nuclear Regulatory Commission (NRC).

[506] See, for example, opening remarks of FCC Commissioners, "Opening Remarks," VoIP Forum, December 1, 2003, http://www.fcc.gov/voip/voipforum.html (accessed January 31, 2008); Werbach, "Digital Tornado," and Oxman, "Unregulating."

[507] Oxman, "Unregulating," 25.

repeatedly asserted that it should and would monitor developments and reserve the right to regulate in the future if market forces should fail and render regulation necessary.

For the NSA, the trend lines in terms of widespread use of personal computers, computer communications software, and later use of the Internet seems to have been quite clear from an early stage. What was less clear was how encryption would necessarily fit into each of these, or when, to what extent, and in what form encryption would become a permanent part of the technological, economic, and social landscape. The adoption of a strategy to try to shape and limit the use of encryption—not preventing it, but instead making it less automatic, less user-friendly, less accessible, and weaker—was an adaptive strategy that left a lot of room for tactical maneuvering.

NSA adaptation

The NSA exhibited considerable tactical flexibility and adaptation in its pursuit of its goal of slowing down commercial encryption. Although one could argue that what the NSA did was to throw the kitchen sink at the problem, which it functionally did, many of the behaviors it exhibited actually required the Agency to overcome deeply ingrained beliefs. Some of the tactics the NSA used were fairly predictable: secrecy orders, intimidation, bureaucratic turf battles (NSF, NIST), changing technical specifications of federal encryption standards (DES) during the federal review process, forbidding export and forcing changes to technical specifications during the export control review process for commercial products (Lotus Notes, Microsoft Windows), pre-publication review of academic papers, and classification of textbooks on cryptography, among others. Less obvious tactics included recruiting bureaucratic allies (FBI, DOJ, law enforcement), petitioning incoming administrations (Clinton administration on Digital Telephony), going public to speak to public audiences, attending academic conferences, reversing policy to actual submit proposals for federal standards (Digital Signature Standard), and coming up with, proactively, 'solutions' such as the Clipper Chip.

Two key organizational characteristics of the NSA were their belief in secrecy (no publicity, no public cooperation with other agencies, minimal oversight) and their rightful ownership of cryptography. Recall that even admitting its own existence was a major step for the NSA. For NSA Director Bobby Inman to appeal to a public audience (admittedly of defense contractors) for the need for support for their favored policy of limiting encryption, much less for

Assistant to the Director Clint Brooks to be advocating a public debate on the Clipper Chip and Digital Telephony, was revolutionary. The NSA had a long history of operating in secrecy, with regulatory capture of key Congressional committees and the backing of the various administrations helping this along. Actively reaching out to FBI and DOJ to convince these law enforcement agencies of a shared interest in containing cryptography, and even pitching it in terms of the other agencies' interests, was therefore also uncharacteristic of the NSA. The fact the NSA allowed (and probably encouraged) the FBI to become the mouthpiece for limits on encryption during the battle over the Clipper Chip and Digital Telephony seems to fit better with the NSA's history. Reaching out to the incoming Clinton administration, too, to sell them on the Digital Telephony and Clipper Chip proposals before they even took office also took a willingness to step outside of the NSA's comfort zone.

Submitting a proposal in response to NIST's request for a Digital Signature Standard (DSS) was actually also a departure from historical behavior for the NSA. Recall that the NSA had refused to submit a proposal during the development process for DES in 1973 on the grounds that the requirement to publish the technical specifications of the standard would give outsiders unacceptable insight into how the NSA thought about cryptography. The NSA's active push for adoption of DSS, and specifically its proposal for DSS, was therefore quite a change in policy. Its cooperation with NIST during this process, given the NSA's history of bureaucratic turf battles over jurisdiction over cryptography, was also arguably adaptive. Certainly it contrasted sharply with the NSA's behavior toward NIST during the aftermath of the passage of the Computer Security Act of 1987, when NSA did some bureaucratic maneuvering around Congress and NIST to ensure itself a seat at any table that was discussing cryptography.

In short, the NSA showed an impressive willingness to work against its own organizational culture in pursuit of its goal of slowing down commercial encryption. The FCC case shows less tactical adaptation, but this is most likely because forbearance by definition requires *inaction,* which leaves little room for tactical adaptation.

Section 2. What Made Foresight Possible?

The similarities between the two agencies may help explain how both were able to exhibit foresight. First, technology was at the center of both organizations' duties, which gave

them incentive to stay aware of and even be proactive about managing emerging technologies.[508] Second, both organizations had extensive experience dealing with emerging technologies. Third, both organizations understood their respective technologies and the environment in which they would operate. They were also sensitive to the limits of that knowledge. That is, they were aware of and acknowledged the technological, economic, political, and social uncertainties surrounding the emerging technologies, and so were able to build flexibility into their policies to allow for adaptation.

Technology as central

Technology plays a central role in mission of both the NSA and FCC. This contrasts with many organizations for which technology is a means to an end; the technology itself is not the objective. Most of the literature on managing and adapting to new technologies focuses on technology as a tool, particularly in the business literature.[509] For example, while many government agencies use computer databases to organize their information, the computers are just a tool. In theory, paper and filing cabinets would accomplish the same goal without seriously impacting organizational interests (if not organizational efficiency). By way of contrast, the FCC is a regulatory agency specifically charged with regulating telecommunications. It must understand new technologies and how they fit into the larger landscape of telecommunications technologies in order to regulate them effectively. A failure to manage the new technologies amounts to a failure at its mission. Viewed from this perspective, the FCC's proactive approach to the management of VoIP seems quite reasonable, and fits with organization theory's predictions about the conditions under which organizations are willing to change.

For the NSA, staying at the cutting edge of technology is a matter of survival and effectiveness. The Agency is an active user and developer of cryptography. Without the best and

---

[508] Contrast this centrality with the more widely written-about subject of organizations and adaptation to new technologies, e.g., the failure of the IRS to update its computer systems. For most government organizations and agencies (and organizations and business more generally), technology is simply a means to an end. The IRS's mission is to collect taxes, not to install computers to better track whether taxes are being paid. The technologies themselves are not key to the mission, much less the actual mission.

[509] See, for example, Michael Tushman and Philip Anderson, eds., *Managing Strategic Innovation and Change: A Collection of Readings* (Oxford University Press, 2004); Peter Weill, *Leveraging the New Infrastructure: How Market Leaders capitalize on Information Technology* (Cambridge: Harvard Business School Press, 1998); Alan Porter and Scott Cunningham, *Tech Mining: Exploiting New Technologies for Competitive Advantage* (Wiley-Interscience, 2004); Nicolas Evans, *Business Innovation and Disruptive Technology: Harnessing the Power of Breakthrough Technology... for Competitive Advantage* (Prentice-Hall, 2002).

fastest computers, the most advanced mathematics, the most sophisticated analysis techniques, the NSA cannot not execute its duty of providing signals intelligence or communications security. That is, without understanding new and emerging technologies, the NSA cannot counter new forms of communication or cryptographic techniques or develop new ones to secure the U.S.'s own communications. The NSA's mission requires a future-oriented outlook with respect to emerging technologies. If anything, this may account for why the NSA funds basic research into mathematics, computer science, physics, electrical engineering, and chemistry as well as applied cryptography: it needs to be aware of both the changes on the leading edge of technology as well as advancements in the foundations of science that affect its work.[510]

The willingness of the NSA to look forward and deal proactively with the growth of commercial encryption seems less surprising if one considers mass market encryption a direct threat to the NSA's ability to perform its core mission of obtaining signals intelligence. Organizational theory predicts that organizations will react very strongly to protect its interests when their core mission or core interests are threatened. However, the theory seems to suggest that action is *reactive,* rather than proactive. The seriousness of the threat may help explain why the NSA was able to overcome this obstacle, and proactively formulate a strategy to offset the threat, rather than simply reacting strongly once the threat had become concrete.

It should be noted, however, that it is not merely the centrality of technology to the agency mission that mattered in both of these cases, but the particular technologies in question. In both cases, they were technologies that fell squarely within the agency's purview and clearly affected their missions directly. Mass market encryption clearly threatened the NSA's ability to perform its mission. VoIP also fell clearly under the FCC's jurisdiction as a telecommunications technology and could potentially alter the entire telecommunications landscape. It is not clear how well either agency would have managed or anticipated emerging technologies that with smaller or less obvious impact on their mission.

Experience with emerging technology

Both the NSA and FCC had long experience in dealing with a series of emerging technologies, and had learned the rather clichéd lesson that change is inevitable and

[510] For example, the NSA funds (and presumably conducts its own) research into quantum cryptography, which is believed to be the next frontier in cryptography.

unpredictable. More importantly, I believe experience had taught them how to better cope with those changes. Specifically, it had taught them not to focus their energies on trying to predict exactly how the technology would develop or on details of specific future scenarios but instead on larger trends and underlying principles. This would allow them to build flexible and adaptive policies to best protect their interests in light of those larger shifts.

Given the overlap in their interest in telecommunications, both organizations found themselves struggling to deal with the changes caused by many of the same technologies, all of which developed rather rapidly in a short period of time. The FCC is an older agency, originally founded to regulate radio, telegraphs and telephones in 1934. In its lifetime, the FCC saw the demise of the telegraph, and the introduction of short wave radio, cable TV, microwave communications, computer communications, satellite communications, cellular phones, broadband, and the Internet, just to name a few technologies. While one could certainly criticize the FCC's handling of any of these technologies, I think it is arguable that very few other government agencies have had to cope with quite so many technological changes in so short a span of time. The NSA, too, dealt with many of the same technologies, even though at its founding in 1952 most of the communications it intercepted were also mostly radio, telephone and telegraph—hardly the digital communications that form the bulk of its work today. The changes both organizations dealt with were not limited to new technologies, of course. Even one of the oldest technologies, the telephone, underwent significant changes when digital switches were introduced, and when those lines, later replaced by fiber, began carrying communications other than telephone calls (faxes, email, computer modems seeking Internet access). The breakup of the Bell monopoly also fundamentally altered the economic landscape for all actors involved.

I believe that the repeated upheavals in technology, when paired with its experiences dealing with politically and economically influential incumbents such as the Bell monopoly, resulted in the FCC's disposition toward a cautious approach in applying regulation. It had learned that it is easier to impose regulation later than to undo regulation imposed too early. Although not explicitly stated, the FCC seemed to recognize that regulation creates stakeholders who have an incentive to organize to protect their interests against newcomers and other threats. (Olsonian collective action) Furthermore, at least some people within the FCC had probably also recognized that it was not immune to the influence of these stakeholders, because its own political structure as a five-member, politically divided Commission and its close cooperation

with industry predisposed it to being 'captured'. (Stigler) The experience of the bungled communications/ data processing framework established during *Computer I*, which had to be abandoned almost immediately, had shown both the value of looking forward (to buy time to anticipate and think) and the hazards of getting regulation wrong (hindering innovation through regulatory confusion). During the period discussed in the VoIP case, the FCC was faced with both rapid technological changes prompted by the Internet as well as an incredibly ambiguous piece of legislation in the 1996 Telecommunications Act. This both presented an obstacle, in that there were no clear guides to action, and an opportunity, because it gave them a lot of leeway in implementing policy, including the legal shield of the Act's "forbearance" clause.

The open historical record for the NSA and how it coped with new technologies is less clear. Obviously, the NSA lived through the same digital revolution that the FCC did. I can only assume from the NSA's continuing reputation as the premier cryptographic agency in the U.S., and arguably the world, that the Agency dealt with all of those new technologies quite successfully, current legal scandals notwithstanding. I would argue that of all the new technologies of the past half century, the introduction of built-in, mass market encryption probably presented the greatest challenge to the NSA's ability to easily obtain communications intelligence, so it was critical that the Agency get its policy right on this issue.

Technical expertise and awareness of limits to knowledge

Both organizations were experts in their respective fields, although their knowledge took different forms. The NSA was an expert developer and user of encryption, and had possibly already trod the technological paths commercial encryption was exploring. The FCC, on the other hand, was certainly competent technically, but its great strength was in understanding the limits of both its technical knowledge and its ability to regulate in a fine-grained way. I believe these qualities helped encourage foresight in two ways. First, technical understanding reduces fear and mistaken understanding of capabilities and consequences of new technologies. Organizational theory suggests that organizations do not like change, and new technologies by definition can force change. Fear and uncertainty increase the resistance to change, so technical understanding alleviates some of that fear. Second, as with historical experience, awareness of uncertainties and limits to knowledge increases caution when organizations do act. In this case,

when combined with historical experience, it pushed the two organizations to adopt flexible strategies that did not depend upon specific predictions.

Section 3. Reasons for Differences in Approach

Despite their similar histories in dealing with a series of emerging technologies, the central role of technology, and even technical expertise, there was clearly a significant difference between the way the NSA and FCC approached management of encryption and VoIP. I believe there are two reasons for this. First, the NSA may have believed that it faced less technological and economic uncertainty than did the FCC. Second, the differing roles of the two organizations, one as a stakeholder in the encryption debate and the other as an ostensibly neutral regulatory agency, created different incentives to action.

The NSA's approach to managing commercial encryption was far more active and hands-on than the policy adopted by the FCC for VoIP. I believe this was in large part due to the lesser technological uncertainty the NSA believed it faced. The NSA was the nation's clear leader in developing cryptographic technology and had been for many decades as a result of its virtual monopoly on cryptography. Given this lead in technical development, it is entirely possible that the NSA believed that it had a good sense for how commercial cryptography would develop, because it was territory the NSA had already covered. The real question, it seemed, was how fast civilian cryptographers could cover that ground. As an NSA official told Whit Diffie, one of the co-discovers of public key cryptography, "It's not that we haven't seen this territory before, but you are covering it very quickly."[511] In this sense, the largest source of uncertainty in emerging technologies, namely how the technology would develop, was actually not as much of an issue for the NSA. Although the NSA had never dealt with mass market cryptography, it did have limited experience dealing with commercial cryptography used by large organizations, such as financial institutions, so commercial cryptography was not an entirely foreign area. (DSD-1, which became DES, had originally been developed by IBM for the financial sector.) This experience and technical understanding may have given the Agency greater confidence in its ability to successfully intervene in technological developments on a micro-level.

The NSA's acknowledged technical expertise also lent it more authority to speak on issues of cryptography, which gave it additional avenues for pursuing its objectives. The most

[511] Diffie and Landau, *Privacy*, 239.

prominent example is how the NSA re-inserted itself in cryptography standards process after Congress gave jurisdiction over civilian cryptography to NIST. The NSA was able to make a compelling argument that its superior resources and technical knowledge should give it a seat at the table.

The FCC, though it had regulatory authority over telecommunications, could not pretend to speak from a position of superior technical knowledge. Instead, the Commission repeatedly sought information and opinions from the various players in telecommunications as new technologies developed. For example, in response to the growing intersection between computers and communications, the FCC opened the *Computer Inquiries*. A similar but smaller-scale effort was launched in the *Broadband Inquiries* as well. The FCC's Inquiry process of soliciting open-ended opinions and analyses about how to better identify and understand the problems that new technologies could bring actually seems to be rather unusual, if not unique, in government.[512] What is common to other government agencies as a matter of administrative law is the comments period for various Notices of Proposed Rulemaking, which is a formal, limited-time process that allows interested actors to comment on proposed regulations. The Commission does not pretend to be technically expert during either of these processes, however; its position at the table is guaranteed because it is the regulatory agency in charge.

Secondly, the NSA had a very different agenda than the FCC. The NSA wanted to *discourage* technological innovation in the commercial sector, whereas the FCC wanted to promote it. As Werbach argued in the OPP working paper, even the most well-intentioned regulators lacked the ability to institute fine-grained regulations without potentially provoking negative consequences, namely distorting the market or hindering innovation. In other words, it is much easier for a government agency to hamper innovation than it is to promote it. Both the political science and business literatures on fostering innovation seem to suggest that there are a million ways to get it wrong, but very few ways to get it right. The NSA just wanted to slow down development and use of cryptography. It did not need a finely calibrated strategy, although a multi-pronged strategy would certainly be more effective. In the export control review process, the NSA had a quite considerable weapon against commercial cryptography, since most

[512] It seems that the FCC's process does have some advantages. It allows the FCC to get a better feel for the positions of incumbent actors. The Inquiry process may also let the FCC harness the brainpower of outside thinkers, who could raise points the FCC may not have considered.

computer software depends upon export markets for profitability. The FCC had a much finer needle to thread in trying to promote VoIP innovation.

Section 4. Other possible explanations, areas for further research

Organizational or Personal Characteristics

In these explanations for the NSA and FCC's ability to show foresight, and in the NSA's case, adaptation, I have largely focused on the organizations' relationship with technology. If I had more time, I would have liked to explore more deeply some of the organizational attributes that might have contributed to both organizations' willingness to look forward and act. First and foremost, I think the question of the organizational structure matters. The existence of a specialized body dedicated to long-range strategic thinking with in the FCC, the Office of Plans and Policy (OPP), seems to have played a central role in developing and reinforcing the policy of forbearance. Clearly, though, the mere existence of an internal think tank is not enough to force an organization to be proactive or flexible in managing emerging technologies; many studies done by internal think tanks are routinely ignored. It would be interesting to see whether the NSA has a similar internal strategic policy think-tank.[513] The case seems to suggest that much of the initiative to pursue a more public strategy came from the top, from the Director (Bobby Inman) or a Special Assistant to the Director (Clinton Brooks).

This raises a follow-up question, then: what was it about the OPP or the FCC that made the Commissioners pay attention to those working papers and incorporate their ideas into policy? The head of the OPP, Robert Pepper, had been at the FCC for a very long time and was widely respected within the industry. Was it his endorsement of those policies that influenced policy-makers? Or was it the papers themselves? The Werbach and Oxman papers were themselves very well written and argued. Was it simply a triumph of rhetoric, a victory for ideas? I find myself somewhat skeptical of this explanation, if only because so many good ideas are ignored – hence why after an accident someone is always able to find a memo somewhere warning that it would happen – that the 'cream rising to the top' seems a rather naively optimistic explanation. Or did the papers or authors themselves have influential champions within the Commission?

---

[513] I have been told by a friend who works closely with the NSA that they have an internal think tank dedicated to technology, but it is not clear that they cover strategic or policy issues, only technical ones. (Dietrich Falkenthal, personal communication, January 9, 2008).

Alternatively, was there something different about the individual Commissioners that predisposed them to a policy of forbearance, to adopting a cautious approach? Did these papers happen to fit in with the general deregulatory ideology that already existed at the Commission, such that they became another justification for a policy already decided upon? For the NSA, was there something special about these particular men, Inman and Brooks, that caused them to be champions for change? Is this a 'great men' story? It seems a question worth exploring, given the unusual nature of both of these cases.

Implementation

A second question focuses on the implementation of strategy. If as organizational theory suggests, organizations resist change, how were the decision-makers able to get the rest of the organization on board? The NSA case shows that many within the Agency resisted Clinton Brooks' urging for a public debate over cryptography, yet one occurred anyway. How did this come to be? At the FCC, by the time VoIP entered the picture, deregulation and laissez faire economics had replaced the old managed monopoly ethos of an earlier era. How did that come to pass? Recognition of the need to look forward is important. Acting upon that recognition, and doing it successfully, are two other steps that both the NSA and FCC seemed to manage, in contrast to the conventional view of government agencies as being slow, unwieldy, and dumb. How was this possible?

The VoIP case presents another question with regards to implementation: how does an organization know when to stop? If the FCC was actively pursuing a policy of forbearance, what was it about the nature of the outside pressure from law enforcement on CALEA, and from Congress and incumbent telcos on the Universal Service Fund, that made the FCC decide to begin regulating? Did this external pressure play a role at all? An alternative explanation, that by 2004 VoIP technology had matured sufficiently to begin regulation, seems plausible. Imposing regulation at any point constrains opportunity (innovation). However, in some sense it also creates opportunities for different forms of innovation, as some of the comments to the FBI petition noted.[514] After all, requiring a CALEA-compliant system drives innovation in at least some subset of the software sector that builds that software. How does a regulatory agency decide when the time is right to begin regulating?

---

[514] Comments of Top Layer Networks, Inc., on *Joint Petition*.

Was I Wrong?

Third, it is possible that the neither the FCC nor the NSA were actually pursuing the forward-looking strategies I attribute to them. If the Commission was simply unprepared to regulate VoIP, it would have used the same politically correct justifications of promoting innovation and fear of premature regulation. The inaction until 2004 could have been a result of political infighting or stalemate among the Commissioners, given the 3-2 political party split of the Commissioners. Regulatory capture by incumbent telcos could have played a role as well, although given the evidence, it seems more likely that the incumbents would have cancelled each other out. For example, while US West sought to have access charges imposed on Class 1 PSTN-IP-PSTN VoIP, AT&T sought to have its Class 1 service declared free from access charges. The Commission chose to ignore the first petition and deny the second, which presumably won it no applause from either petitioner. The only theoretical explanation that fits, other than the FCC pursuing a policy of forbearance, is that the Commission was trying to preserve its bargaining power (regulatory discretion). To some extent, its assertion of the interstate nature of VoIP thereby its authority over VoIP fit with this model of holding on to (and even expanding) regulatory power. The issue certainly warrants further exploration.

For the NSA, the tactical adaptation used to slow down deployment of mass market encryption could also be explained as desperation. One could view the Agency's 'kitchen sink' approach as indicative of a lack of strategy at all, in pursuit of the very old and now unattainable goal of putting the encryption genie back in the bottle. I do not believe this is the case, however. Organizations that are trying to prevent change tend to do more of the same. Working against organizational culture to the extent that the NSA did is unusual, painful even, and unlikely to occur except very deliberately. Moreover, the NSA virtually disappeared from the front lines of the encryption debate during the 1990s. I think they had decided by that point to focus their attentions on building up their own capabilities to mitigate the effects of mass market encryption rather than try to stop it through political means. As a last resort, as we have seen in the scandal over NSA warrantless wiretapping in the past two years, clearly the NSA does not need the Clipper Chip or CALEA in order to intercept communications—those would make it easier, and more politically palatable, but the lack of either initiative did not make eavesdropping impossible.

Conclusion

Despite the conventional view of organizations, and particularly government bureaucracies, as being reactive and resistant to change, both the NSA and FCC showed foresight and policy flexibility in their management of mass market encryption and VoIP technologies, respectively. The importance of technology to each organization's mission helped motivate them to take a proactive approach to emerging technology. Experience in dealing with other emerging technologies had taught both organizations that flexible policies that took into account the general direction of change would be more useful than trying to predict the precise form of uncertainty. Lastly, both organizations leveraged their particular technical expertise, with a sensitivity to the limits of knowledge, in order to formulate policies to manage the uncertainties that new technologies would bring.

Chapter 5
Conclusion

In this final chapter I would like to take a step back from the two cases explored in this dissertation, and ask not just what we have learned, but what we can learn. This chapter is roughly divided into two halves. The first covers flaws in this study and potential avenues for future research. The second discusses the policy implications of the findings from this study and flags an issue not directly related to technology policy that came up during the course of my research.

This dissertation has sought to understand when government agencies exhibit foresight and adaptation in formulating and executing strategies for managing emerging technologies. We have seen that the stereotype of government agencies as being reactive and slow to change is not true of either the NSA or FCC in their management of mass market encryption and VoIP technologies, respectively. Both agencies showed a considerable willingness to anticipate the changes their respective emerging technologies would bring to the political, social, economic, and technological environments, and pursued flexible strategies to manage those technologies. The NSA proved itself willing to adapt tactically, even to the extent of acting against an organizational culture of closure and secrecy, in pursuit of its encryption management strategy. The FCC, for its part, adopted a fairly unusual strategy of regulatory restraint in order to promote the growth of VoIP.

The previous chapter postulated that the NSA and FCC showed foresight because of their prior experience dealing with emerging technologies, their technical expertise and sensitivity to the limits of that expertise, and the central role of technology in their organizational missions. The differences in their approaches seemed to stem from differing levels of perceived technological uncertainty, and more importantly, the different objectives each agency had with respect to the development (or lack thereof) of their particular technology. The latter reason is largely a function of the differing roles of the two agencies: the NSA, as a functional agency, has an active interest in encryption, whereas the FCC, as a regulatory agency, is at least theoretically neutral.

Future Research

This brings me to first issue I hope to cover in this chapter: that of how to improve and expand upon the research in this dissertation. As I stated in the introduction, the evolving focus of this dissertation meant that the two cases were not optimally comparable. What needs to be done is to expand the number of cases, thereby increasing the variation on both the independent and dependent variables. Although not by design, both the NSA and FCC showed foresight. It would be useful to look at cases when agencies *failed* to show foresight or adaptation as well, which could give valuable insight into which variables and conditions matter most for spurring foresight and adaptation.

On the independent variable side, there are areas of non-comparability between the NSA and FCC I would like to explore further, in order to tease out how much influence they had on the current findings. First, the functional vs. regulatory agency issue may have increased the NSA's incentive to actively manage mass market encryption. I would like to look at more agencies to see if this pattern holds true, perhaps limiting the initial probe to regulatory agencies with a focus on technology, such as the Food and Drug Administration (FDA), the Nuclear Regulatory Commission (NRC), the Environmental Protection Agency (EPA), and Occupational Safety and Health Administration (OSHA). The study could then be expanded to include technology-focused functional agencies, such as the National Aeronautics and Space Administration (NASA) and the National Reconnaissance Office (NRO). During this case selection, I would like to remain sensitive to the fact there are many different types of government agencies, whether independent, belonging to a particular branch of government, or a wholly separate board or commission, which may also influence their actions.[515]

Second, I would like to further investigate the influence of dual-use versus 'regular' technologies upon my findings. Encryption policy had to consider national security concerns very seriously. National security is rightly considered a priority in federal policy, but its importance may also have skewed the NSA's incentives toward hypervigilance—which I may be interpreting as foresight. Examining a greater range of both regular and dual-use technologies could help settle this question.

---

[515] Louisiana State University Federal Agencies Directory website, http://www.lib.lsu.edu/gov/fedgov.html (accessed January 9, 2008).

Third, further exploration of the organization's leadership structure variable—namely whether the agency has a unitary leader or is led by a commission—would help answer the question of whether the FCC's forbearance was not simply a product of political stalemate. Clearly, I do not believe it was, but political deadlock may have helped prevent (premature) action, in contrast to the NSA's unitary leadership and its very active management of encryption. It would also be interesting to see whether policy decisions that require foresight are executed more quickly or decisively in one type of organization versus another.

Further research with more cases would also help answer some of the other questions that arose in the course of this research. First and foremost, it would help answer the question of why the outcomes of these two cases differed so much from what conventional wisdom might expect. Is it simply that conventional wisdom is wrong? Do most organizations actually show foresight, but no one has investigated closely and so no one knows? Certainly I would not have predicted before starting this research that both the NSA and FCC, the first with a reputation for being an impenetrable monolith and the latter for being a three-ring political circus, would turn out to be quite flexible and innovative. Did I just happen to choose two extremely unusual cases? Or does conventional wisdom only function for certain cases, under certain conditions? And if so, what are they?

Second, looking at more cases would help establish a baseline for forbearance. The FCC's policy of forbearance, of actively and deliberately refraining from regulation, seems to catch everyone's attention because it runs so contrary to the conventional view of bureaucracies as self-aggrandizing institutions. Do other agencies also forbear from regulating, and if so, why?

Third, a greater number of data points would help answer a question that I personally find quite interesting: how unique is the FCC's Inquiry process? Administrative law requires federal agencies to post notices of proposed rule-making and to allow for comments. This is a time-consuming process, but by all indications, agencies take it very seriously and do read and deliberate over all of the comments they receive.[516] However, large-scale, multi-year inquiries into broad questions such as the regulatory and policy questions generated by the convergence of computers and communications, which were the topic of the *Computer Inquiries,* seem rare. Yet

[516] The FCC references many of the Comments and Reply to Comments and other submissions in each progressive report they issued in the CALEA and IP-Enabled Services dockets, which suggests that someone has been reading the Comments quite carefully.

these types of investigations are precisely those that would help an organization map its way into the future with adequate sensitivity to uncertainty. Do other agencies conduct such studies? If not, why not?

Policy Implications

The second topic I would like to cover in this chapter is the policy implications of this dissertation. Overall, based on my research, I am not optimistic about the ability of most government agencies to show foresight in managing emerging technologies. Although I happened upon two quite successful cases, it seems the conditions for success that I identified do not hold true for most agencies, much less for most situations. The centrality of technology to an organization's mission either exists or it does not. Technical expertise is difficult and expensive to develop. A history of working with emerging technologies does not always exist, either. Even if an agency has such a history, it is not clear that it will draw the same lessons from those experiences that the NSA and FCC did. That is, its experiences may not predispose it toward formulating flexible policy or recognizing the limits of their knowledge, which can be humbling. Nor does it mean the agency will recognize the need to manage for uncertainty rather than trying to predict the future. Lastly, most agencies, particularly regulatory agencies, will most likely have to foster rather than stifle innovation, and the former is by far the more difficult task.

The picture is not wholly negative, however. At least two of the conditions can be learned. Namely, the agencies can create awareness of the need for flexible policies. They can also encourage awareness of the limits of knowledge, and a greater sensitivity to knowing what is unknown. In addition, although expensive, technical expertise can be built, or contracted from outside. Hopefully these efforts will be enough to offset the difficulties noted above, and to move agencies toward more proactive technology management policies.

The last issue I want to flag is not directly related to technology management, although I first noticed it while researching the encryption case, and it came up again through current events during my research on the VoIP case. The issue is that national security arguments tend to dominate other arguments when external threats are perceived, regardless of the validity of the actual argument.

Theories of public policy suggest that policy entrepreneurs and agenda setters are sensitive to the external political environment.[517] Policy entrepreneurs and agencies seeking to advocate existing solutions exploit changes in the external environment to their respective agendas. From looking at the encryption and VoIP cases, it seems particularly true that when external security threats are perceived, as during the height of the Cold War or after September 11, 2001, any argument that can be framed in terms of national security seems to carry more weight. Other values, such as civil liberties and economic interests, seem to fall by the wayside when national security concerns dominate. However, when perceived external security threats are smaller, those values bubble up to the top of the agenda.

The prioritization of arguments framed in terms of national security may hold true regardless of whether those arguments can be backed up by facts. That is, they seem to be less closely examined in times of perceived threat. For example, during the 1980s the NSA insisted upon maintaining strict export controls over DES chips, even though the algorithm was widely available outside of the U.S.. In 2004, law enforcement agencies argued that criminals *and terrorists* were using VoIP because they knew it could not be wiretapped, and so VoIP should be subjected to CALEA requirements. However, when challenged to produce evidence of instances in which that had happened, FBI could not, yet the FCC seemed to accept the argument anyway.[518] The inclusion of "terrorists" in the justification for expansion of CALEA obligations is noteworthy mostly because it reflects how preferred policies are repackaged in response to the external political climate. CALEA had not changed between 1994 and 2004. However, the perceived threat had: after September 11, marketing preferred policies as "counter-terrorism measures" was a way to get attention and funding, and so a law that had never mentioned terrorists became a counter-terrorism initiative overnight.

At the same time, concerns for civil liberties or economic development become less pressing when national security arguments dominate. During the 1990s, after the Cold War

---

[517] See John Kingdon, *Agendas, Alternatives and Public Policies* (Boston: Little, Brown, 1984), on windows of opportunity and the need for a problem, solution, and policy entrepreneur to all be in the right place at the right time for action to happen; this is a refinement of the classic Michael D. Cohen, James G. March, Johan P. Olsen, "A Garbage Can Model of Organizational Choice," *Administrative Science Quarterly* 17:1 (March 1972): 1-25; Anthony Downs, "Up and Down with Ecology: The Issue Attention Cycle," *The Public Interest* 28 (Summer 1972): 38-50, responses to crisis restarts the agenda, and public attention rarely remains focused.

[518] As far as I know, there have been no documented cases in the U.S. where the FBI or law enforcement has been unable to wiretap due to the target's use of VoIP. The first instance internationally apparently occurred in December 2006, when the German authorities wiretapped a man who was using Skype. The police completed the wiretap, but could not decrypt the encrypted communication. (Chintan Vaishnav, personal communication, December 20, 2006).

ended, economics and civil liberties concerns became more important in relative terms. For example, when the first Digital Telephony proposal was submitted in 1992, Congress rejected it in part because of the cost concerns of telecommunications carriers, which objected to the FBI's proposal that all costs of CALEA implementation be borne by the carriers. A decade later, after September 11, 2001, when the law enforcement agencies again proposed that carriers shoulder the costs of VoIP-CALEA compliance, the FCC sided with law enforcement. In the 1990s, one of the many reasons the Clipper Chip initiative failed was because the FBI could not explain why criminals would actually use Clipper-encrypted devices. A decade later, law enforcement's inability to produce evidence of criminals and terrorists using VoIP to circumvent traditional wiretapping did not seem to concern the FCC. The law enforcement agencies again had no response to the question of why criminals and terrorists would not simply use non-U.S. based facilities that were not subject to CALEA, or why they would not encrypt their communications to make the wiretap more difficult.

The general lack of emphasis put on civil liberties after September 11, and particularly in the current uproar over the NSA's warrantless wiretapping and the complicity of telecommunications providers, has historical precedent. There are many similarities between the domestic surveillance conducted in the 1970s and today. As with the current situation, the *New York Times* broke the story. The revelation led to Congressional investigations in 1975. The Church Committee investigated abuses by the intelligence community and found that the FBI, CIA, IRS, and NSA had all conducted domestic surveillance of U.S. citizens.[519] The Committee also discovered that a former Nixon White House aide and a former Director of the NSA had advocated using the capabilities of the NSA to conduct domestic surveillance against antiwar protestors and those opposed to the views of the administration (the Huston Plan).[520] The NSA maintained a "watch list" of U.S. citizens, and had conducted surveillance of their foreign communications.[521]

Another project, codenamed Shamrock, involved the cooperation of the major telegraph companies (RCA Global, ITT World Communications, and Western Union International) in

---

[519] Church Committee Reports, http://www.aarclibrary.org/publib/church/reports/contents.htm (accessed January 8, 2008). See especially Volume 5 ("The National Security Agency and Fourth Amendment Rights").
[520] Church Committee Reports, Vol. 2 ("Huston Plan").
[521] Church Committee Reports, Vol 2. ("Huston Plan") and Vol. 5, 1-5. See also Katelyn Epsley-Jones and Christina Frenzel, "The Church Committee Hearings & and the FISA Court," http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/churchfisa.html;

providing access to copies of all telegrams leaving New York, which the NSA copied onto tape and archived.[522] The program actually predated the establishment of the NSA, a holdover from wartime surveillance conducted by the Army Security Agency that had simply continued unquestioned when the NSA was established. All three companies asserted that they had been asked, without proof of legal authority, to provide access to domestic communications, and that they had cooperated without receiving compensation from the government in the belief that they were helping to protect national security.[523] As is the case today, both the NSA and the Congressional Committee sought to protect those companies from legal repercussions of their actions, because exposing them to embarrassment and lawsuits would discourage other companies from cooperating in the future. They argued that technology made surveillance impossible without the telcos' cooperation, echoing the sentiments of the current NSA Director.[524] Also like today, the former deputy director of the NSA at the time, Louis Tordella, stated that most of those communications were never read, except when particular names were flagged. The current debate over the Bush administration's granting of immunity to the telecom companies that cooperated with the NSA shares disturbing similarities with the Cold War era domestic surveillance, all done in the name of national security.[525]

The Church Committee resulted in the passage of the Foreign Intelligence Surveillance Act (FISA) of 1978, which created the secret Foreign Intelligence Surveillance Court to issue warrants for domestic surveillance. The intent was to create some sort of check on the ability of intelligence agencies to conduct unauthorized surveillance. As the recent scandal over warrantless wiretapping shows, however, clearly even that check can be circumvented. The

---

[522] L. Britt Snider, "Recollections from the Church Committee's Investigation of NSA," https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art4.html (accessed January 7, 2008).

[523] See Ellen Nakashima, "A Story of Surveillance," *Washington Post,* November 7, 2007, D1.

[524] Eric Lichtblau, James Risen and Scott Shane, "Wider Spying Fuels Aid Plan for Telecom Industry," *New York Times,* December 16, 2007, http://www.nytimes.com/2007/12/16/washington/16nsa.html?ex=1355461200&en=a6aa871994ebe9e8&ei=5090&partner=rssuserland&emc=rss (accessed January 8, 2008), which argues that changes in technology are the reason that the NSA must have the cooperation of telcos;
See also op-ed by Mike McConnell, current director of the NSA: Mike McConnell, "Help Me Spy on Al Qaeda," *New York Times,* December 10, 2007.

[525] David Stout, "Telecom Industry Wins a Round on Eavesdropping," New York Times, December 17, 2007, at http://www.nytimes.com/2007/12/17/washington/17cnd-nsa.html?ex=1355547600&en=616ba05a32ffabf9&ei=5088&partner=rssnyt&emc=rss; Jonathan Weisman and Paul Kane, "Telecom Immunity Issue Derails Spy Law Overhaul," *Washington Post,* December 17, 2007, A02; http://news.yahoo.com/s/nm/20071217/pl_nm/usa_security_phones_dc_1;_ylt=AlvXnEKTDTrMAK__JiHcIsYE1vAI (both accessed January 8, 2008).

recent update, named the Protect America Act of 2007, expands the powers of the NSA to conduct domestic surveillance even more.[526]

I am not sure what all of this means for the future of Fourth Amendment rights. I can say that we seem to have come full circle in thirty years, returning to an era when fear, cloaked in the mantle of preserving national security, overruled civil liberties despite earlier attempts to prevent just such a thing from happening. I can only hope that this time we install better safeguards against such abuses.

[526]Declan McCullagh and Anne Broach, "FAQ: How far does the new wiretap law go?" CNET News.com, August 6, 2007, http://www.news.com/FAQ-How-far-does-the-new-wiretap-law-go/2100-1029_3-6201032.html?tag=sas.email (accessed January 31, 2008).

Bibliography

General References

---. "A Discussion of RSA-129 Activity," http://www.math.okstate.edu/~wrightd/numthry/rsa129.html (accessed February 3, 2008)

"Reactive vs. Proactive Change." http://www.referenceforbusiness.com/management/Pr-Sa/Reactive-vs-Proactive-Change.html (accessed January 6, 2008)

Abbate, Janet. *Inventing the Internet.* Cambridge: MIT Press, 1999.

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

AT&T, "History," www.att.com/history (accessed August 3, 2007)

Atkinson, Robert. "Internet Telephone Service: A New Era of Competition in Telecommunications." Policy Report. Progressive Policy Institute. March 2005. http://www.ndol.org/documents/VoIP.pdf (accessed January 26, 2008).

Bamford, James. *Puzzle Palace.* Boston: Houghton-Mifflin, 1989.

Bellovin, Steven, Matt Blaze, et al. "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP." Paper for the Information Technology Association of America. http://www.itaa.org/news/docs/CALEAVOIPreport.pdf (accessed August 3, 2007).

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

Bowersox, Joe. *The Moral Austerity of Environmental Decision Making: Sustainability, Democracy, and Normative Argument in Policy and Law.* Duke University Press, 2002.

Brooks, Clinton C. Memo. April 28, 1992. Reprinted in *Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance,* edited by David Banisar and Bruce Schneier, C8-C13. New York: Wiley and Sons, 1997.

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

Chadbourne & Parke LLP, "Client Alert: AT&T Seeks FCC Ruling Exempting IP Telephony from Access Charges," http://www.chadbourne.com/files/Publication/4cdea554-a5b2-4d1b-9a15-82b6c468d525/Presentation/PublicationAttachment/95745a71-6def-42b0-80dd-8318534a9a71/AT&TSeeksFCCRulingExemptingIPTelephonyfromAccessCharges.pdf (accessed January 31, 2008).

Chandra, Vandana. *Technology, Adaptation, and Exports: How Some Countries Got It Right* (World Bank Publications, 2006).

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

Clark, David D. "A Taxonomy of Internet Telephony Applications." In *Internet Telephony,* eds. Lee W. McKnight, William Lehr, and David D. Clark. Cambridge, MA: MIT Press, 2001.

Clark, David D. Personal communication. December 21, 2007.

Cohen, Michael D., James G. March, Johan P. Olsen. "A Garbage Can Model of Organizational Choice." *Administrative Science Quarterly* 17:1 (March 1972): 1-25.

Cybertelecom.org, "AT&T AntiTrust," http://www.cybertelecom.org/notes/att_antitrust.htm#ant3 (accessed August 3, 2007).

---, "Common Carriers," http://www.cybertelecom.org/notes/common_carrier.htm (accessed August 3, 2007).

---, "Communications Act of 1934," http://www.cybertelecom.org/notes/communications_act.htm (accessed August 3, 2007).

---. "ACTA Petition," http://www.cybertelecom.org/voip/acta.htm (accessed August 3, 2007).

Dam, Kenneth 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.* Washington, D.C.: National Academy Press, 1996.

Davida, George. "The Case Against Restraints on Non-governmental Research in Cryptography." *Cryptologia* 5 (July 1981): 143.

Diffie, Whitfield, and David Landau. *Privacy on the Line.* Cambridge, MA: MIT Press, 1998.

Diffie, Whitfield, David Landau and Gina Bari Kolata. "Computer Encryption and the National Security Agency Connection." *Science* 97. (July 29, 1977): 438-40

Downs, Anthony. "Up and Down with Ecology: The Issue Attention Cycle." *The Public Interest* 28 (Summer 1972): 38-50.

Dursht, Kenneth A. "From Containment to Cooperation: Collective Action and the Wassenaar Arrangement." 19 *Cardozo Law Review* 3 (December 1997): 1079-1123.

Electronic Privacy Information Center. *Cryptography and Liberty 1999: An International Survey of Encryption Policy.* Washington, D.C.: EPIC, 1999.

Epsley-Jones, Katelyn, and Christina Frenzel. "The Church Committee Hearings & and the FISA Court." http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/churchfisa.html (accessed January 7, 2008).

Epstein, David and Sharyn O'Halloran. *Delegating Power: A Transaction Cost Politics Approach to Policy Making under Separate Powers.* Cambridge: Cambridge University Press, 1999.

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

Evans, Nicolas. *Business Innovation and Disruptive Technology: Harnessing the Power of Breakthrough Technology... for Competitive Advantage.* Prentice-Hall, 2002.

Falkenthal, Dietrich. Personal communication. January 9, 2008.

Federal Communications Commission. "Universal Service." http://www.fcc.gov/wcb/tapd/universal_service/ (accessed January 3, 2008).

Feistel, Horst. "Cryptography and Computer Privacy." *Scientific American* 228 (May 1973): 15-23.

Freeh, Louis. "Speech to American Law Institute, May 19, 1994." Reprinted in *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls*. Electronic Privacy Information Center, *6.* Upland, PA: Diane Publishing Co., 1994.

Garfinkel, Simson. *PGP.* (Cambridge: O'Reilly and Associates, 1995),

Halstuk, Martin. "Rights v. Privacy: A Pending Case May Open a Back Door to Prior Restraint." *Columbia Journalism Review* 2003, http://cjrarchives.org/issues/2003/1/privacy-halstuk.asp (accessed January 15, 2008).

Harmon, John M. "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 Lance Hoffman, *Building in Big Brother* (New York : Springer-Verlag, 1995).

Hung, Shirley K. "U.S. Export Controls on Encryption Technology." Master's thesis, Massachusetts Institute of Technology, 2004.

Inman, Robert. "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector." Reprinted in *Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance,* Edited by David Banisar and Bruce Schneier, 347. New York: Wiley and Sons, 1997.

Internet Engineering Task Force (IETF). "Sessions Initiation Protocol (sip) Charter." http://www.ietf.org/html.charters/sip-charter.html (accessed February 1, 2008).

Internet Society. "Internet History." http://www.isoc.org/internet/history/brief.shtml (accessed August 11, 2007).

Jones, William. "The Common Carrier Concept as Applied to Telecommunications: A Historical Perspective." http://www.cybertelecom.org/notes/jones.htm (accessed August 3, 2007).

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

Kamieniecki, Sheldon. *Corporate America and Environmental Policy: How Often Does Business Get Its Way?* Palo Alto: Stanford University Press, 2006.

Kingdon, John. *Agendas, Alternatives and Public Policies.* Boston: Little, Brown, 1984.

Kruh, Louis. "Cryptology and the Law–VII." *Cryptologia* 10 (October 1986): 248.

Landquist, Eric. "The Quadratic Sieve Factoring Algorithm." December 14, 2001, http://www.math.uiuc.edu/~landquis/quadsieve.pdf (accessed February 3, 2008).

Levin, Staci. "Who are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls?" *Law and Policy in International Business* 30 (Spring 1999).

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

---. "The Open Secret," *Wired,* April 1999, http://www.wired.com/wired/archive/7.04/crypto.html (accessed January 21, 2008)

---. *Crypto.* New York: Viking, 2001.

Louisiana State University Federal Agencies Directory website, http://www.lib.lsu.edu/gov/fedgov.html (accessed January 9, 2008).

Lubbers, Jeffrey. E-mail communication. December 18, 2006.

McCraw, Thomas K. "Regulation in America: A Review Article." *The Business History Review* 49 (Summer 1975): 159-182.

McMaster, Mike. "Foresight: Exploring the Structure of the Future." *Long Range Planning*. 29:2 (1996): 149-55.

McNulty, F. Lynn. "Encryption's Importance to Economic and Infrastructure Security." *Duke Journal of Comparative and International Law* (Spring 1999) .

---. "Memo for the Record, August 18, 1992." Reprinted in *1996 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls.* Electronic Privacy Information Center, C14-C19. Upland, PA: Diane Publishing Co., 1996.

Meese, Edwin and David F. Forte, eds.. *Heritage Guide to the Constitution.* Regency Publishing, Inc., 2006.

Mohammed, Emir A. "The Growth of Internet Telephony: Legal and Policy Issues." *First Monday* http://www.firstmonday.org/issues/issue4_6/mohammed/index.html#m3 (accessed August 3, 2007).

Park, E. John. "Protecting the Core Values of the First Amendment in an Age of New Technologies: Scientific Expression vs. National Security." 2 *Virginia J. of Law and Technology*. 3 (1997).

National Telecommunications and Information Agency. "Technological Competitiveness and Policy Concerns." Reprinted in *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls.* Edited by David Banisar, Electronic Privacy Information Center. Upland, PA: Diane Publishing Co., 1994.

Noam, Eli M. "Beyond Liberalization II: The Impending Doom of Common Carriage." 18 *Telecommunications Policy* 435. Sec. II (1994), http://www.columbia.edu/dlc/wp/citi/citinoam11.html (accessed August 3, 2007).

Nuechterlein, Jonathan E. and Weiser, Philip J. *Digital Crossroads: American Telecommunications Policy in the Internet Age.* Cambridge, MA: MIT Press, 2005.

Olson, Mancur. *The Logic of Collective Action.* Cambridge: Harvard University Press, 1965.
Organization for Economic Cooperation and Development Staff, *Social Sciences and Innovation* (OECD, 2001).

Organization for Economic Cooperation and Development. "Cryptography Policy Guidelines." March 27, 1997, http://www.oecd.org/document/11/0,3343,en_2649_201185_1814731_1_1_1_1,00.html (accessed February 3, 2008).

Organization for Economic Cooperation and Development. "OECD Broadband Portal," http://www.oecd.org/sti/ict/broadband (accessed December 3, 2007).

Oxman, Jason. "The FCC and the Unregulation of the Internet." Federal Communications Commission Office of Plans and Policy Working Paper Series 31, July 1999.

Patrick I. Ross, "Computer Programming Language: Bernstein v. United States Department of State," 13 *Berkeley Technological Law Journal* 305 (1998).

Patrick Ryan, Tom Lookabaugh, and Douglas Sicker, "A Model for Emergency Service of VoIP Through Certification and Labeling," 58 *Federal Communications L.J. (2006)* 116, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=876052

Pepper, Robert. Telephone interview. October 12, 2006.

Porter, Alan, and Scott Cunningham, *Tech Mining: Exploiting New Technologies for Competitive Advantage.* Wiley-Interscience, 2004.

Rivest, Ron, 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.

Saundersby, Kurt M. "The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff." 17 *John Marshall J. of Computer and Information Law* 945 (1999).

Schein, Edgar. "Coming to a New Awareness of Organizational Culture." *Sloan Management Review* 25 (Winter 1984): 3-16.

Schulzrinne, Henning. "Internet telephony." *IEEE Network* 13 (May/June 1999): 6-7, http://ieeexplore.ieee.org/iel5/65/16630/00767131.pdf?arnumber=767131 (accessed August 11, 2007).

---. "SIP: Session Initiation Protocol," at http://www.cs.columbia.edu/sip/ (accessed February 1, 2008).

Session Initiation Protocol (SIP) Working Group. "SIP WG Supplemental Homepage." http://www.softarmor.com/sipwg/ (accessed February 1, 2008).

Shapley, Deborah. "DOD Vacillates on Wisconsin Cryptography Work." *Science* 201 (July 14, 1978): 141.

---. "NSA Slaps Secrecy Order on Inventors' Communications Patent." *Science* 201 (September 8, 1978): 891-94

Shehadeh, Karim K. "The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests." 15 *American University International Law Review* 271 (1999).

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

Singleton, Solveig. "Encryption Policy for the 21st Century: A Future Without Government-Prescribed Key Recovery." Policy Analysis Paper No. 325. Cato Institute. November 19, 1998. http://www.cato.org/pubs/pas/pa325.pdf (accessed January 31, 2008).

Snider, L. Britt. "Recollections from the Church Committee's Investigation of NSA." https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art4.html (accessed January 7, 2008).

Stigler, George. "The Theory of Economic Regulation." *Bell Journal of Economics and Management Science* II (Spring 1971): 3-21.

---. "The Process of Economic Regulation." *The Antitrust Bulletin* XVII (Spring 1972): 207-235.

Sweet, Alec Stone and Mark Thatcher. *The Politics of Delegation.* Routledge, 2004.

Tushman, Michael, and Philip Anderson, eds. *Managing Strategic Innovation and Change: A Collection of Readings.* Oxford University Press, 2004.

Vaishnav, Chintan. "Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation." Master's thesis, Massachusetts Institute of Technology, 2006.

---. Personal communication. December 20, 2006.

van Evera, Stephen. "Why States Believe Foolish Ideas: Non-Self-Evaluation by States and Societies." Unpublished paper. Department of Political Science, Massachusetts Institute of Technology.

Weill, Peter. *Leveraging the New Infrastructure: How Market Leaders capitalize on Information Technology.* Cambridge: Harvard Business School Press, 1998.

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

Werbach, Kevin. "Digital Tornado: The Internet and Telecommunications Policy." Federal Communications Commission Office of Plans and Policy Working Paper Series 29, March 1997.

West, William. "The Politics of Administrative Rulemaking." *Public Administration Review* 42 (September-October 1982): 420-6.

Whitt, Richard S. "A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model." 56 Indiana Journal of Law (2004), http://law.indiana.edu/fclj/pubs/v56/no3/Whitt%20Final%202.pdf (accessed January 26, 2008).

Wildavsky, Aaron. "The Self-Evaluating Organization." *Public Administration Review* 32:5 (Sept.-Oct. 1972): 509-520.

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

Wilson, James Q. "The Dead Hand of Regulation." *Public Interest* 25 (Fall 1971): 54-78.

---. "The Politics of Regulation." In *The Politics of Regulation*, edited by James Q. Wilson, 357-394. NY: Basic Books, 1980.

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

Wilson, Kevin G. *Deregulating Telecommunications: U.S. and Canadian Telecommunications, 1840-1997.* Lanham, MD: Rowman & Littlefield Publishers, 2000.

Wood, J.V. "UK Foresight Programme—A Panel Chairman's View," http://www.nistep.go.jp/achiev/ftx/eng/mat077e/html/mat0774e.html (accessed January 6, 2008)

FCC Documents
(In Chronological Order)

Second Computer Inquiry, *Final Decision*, 77 FCC2d 384, 387.

America's Carriers Telecommunications Association. *Petition.* In the Matter of the Provision of Interstate and International Interexchange Telecommunications Service via the "Internet" by Non-Tariffed, Uncertified Entities. http://www.fcc.gov/Bureaus/Common_Carrier/Other/actapet.html (accessed October 28, 2007).

Public Notice. Common Carrier Bureau Clarifies and Extends Request for Comment on ACTA Petition Relating to "Internet Phone" Software and Hardware. 12 FCC Rcd 15982 (March 25, 1996), http://www.fcc.gov/Bureaus/Common_Carrier/Public_Notices/1996/da960414.txt (accessed August 3, 2007).

Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended. CC Docket No. 96-149. *First Report and Order and Further Notice of Proposed Rulemaking.* 11 FCC Rcd 21905, 21957-58 (1996).

Notice of Proposed Rulemaking. Communications Assistance for Law Enforcement Act. FCC 97-356. Docket No. 97-213. (October 2, 1997). http://askcalea.net/fcc/docs/fcc97356.pdf (accessed February 3, 2008).

Further Notice of Proposed Rulemaking. Communications Assistance for Law Enforcement Act. FCC 98-282. (October 22, 1998) http://www.askcalea.net/fcc/docs/fcc98282.pdf (accessed February 3, 2008).

Memorandum Opinion and Order. FCC 98-233. (September 10, 1998). http://www.fcc.gov/Bureaus/Wireless/Orders/1998/fcc98223.pdf (accessed February 3, 2008)

Notice of Proposed Rulemaking. Appropriate Framework for Broadband Access to the Internet over Wireline Facilities Universal Service Obligations of Broadband Providers. FCC 02-42, Docket No. 02-33 (February 15, 2002).

FCC Commissioners. "Opening Remarks." VoIP Forum. December 1, 2003. http://www.fcc.gov/voip/voipforum.html (accessed January 31, 2008

*Memorandum Opinion and Orde*r. Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, 19 FCC Rcd 3307, ¶ 9 (February 19, 2004)

Federal Bureau of Investigation, Department of Justice, and Drug Enforcement Agency. *Joint Petition for Expedited Rulemaking Concerning the Communications Assistance for Law Enforcement Act.* FCC RM-10865. http://www.askcalea.net/pet/docs/20040310.calea.jper.pdf (accessed January 20, 2008).

Comments on *Joint Petition for Expedited Rulemaking Concerning the Communications* submitted by:
American Association of Community Colleges
American Civil Liberties Union
BellSouth
Cellular Telecommunications and Industry Association
Center for Democracy and Technology
Concerned CALEA Compliant Carriers,
Covad Communications
Electronic Frontier Foundation
Electronic Privacy Information Center
Global Crossing North America, Inc.
Internet Commerce Coalition

ISP Internet Coalition
Leap Wireless
Los Angeles Country Regional Criminal Information Clearinghouse
National Narcotic Officers Association Coalition
National Sheriffs' Association
New York State Police
Rural Iowa Independent Telephone Association
SBC
Skype,
Top Layer Networks, Inc.
United States Telecom Association
US Telecommunications Association
VON Coalition

Order, Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, 19 FCC Rcd 7457 (April 14, 2004), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-97A1.pdf (accessed August 11, 2007).

Notice of Proposed Rulemaking. IP-Enabled Services. FCC 04-36, RM-10865, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-28A1.pdf (accessed January 31, 2008).

News Release. IP-Enabled Services Notice of Proposed Rulemaking. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243868A1.pdf (accessed January 31, 2008).

Notice of Proposed Rulemaking. Communications Assistance for Law Enforcement Act and Broadband Access and Services. FCC 04-187, Docket No. 04-295 (August 4, 2004), http://www.techlawjournal.com/agencies/calea/20040809nprm.pdf (accessed January 20, 2008).

Memorandum Opinion and Order, Vonage Holding Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission, 19 FCC Rcd 22404 (November 9, 2004).

News Release. Commission Requires Interconnected VoIP Providers to Provide Enhanced 911 Service (May 19, 2005), http://fjallfoss.fcc.gov/edocs_public/openAttachment.do?link=DOC-258818A1.pdf (accessed October 20, 2007).

First Report and Order and Notice of Proposed Rulemaking, FCC 05-116 (May 19, 2005), ¶1, http://www.fcc.gov/cgb/voip911order.pdf (accessed October 20, 2007)..

First Report and Order and Notice of Proposed Rulemaking, IP-Enabled Services, E911 Requirements for IP-Enabled Service Providers, 20 FCC Rcd. 10245, (May 19, 2005), http://www.fcc.gov/cgb/voip911order.pdf (accessed February 1, 2008).

First Report and Order and Further Notice of Proposed Rulemaking. Communications Assistance for law Enforcement Act and Broadband Access and Services. FCC 05-153, ET Docket No. 04-295, RM-10865. (August 5, 2005), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf (accessed January 31, 2008).

News Release. FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps. August 5, 2005. http://www.askcalea.net/archives/docs/20050805-fcc-wiretaps.pdf (accessed January 31, 2008).

Report and Order and Notice of Proposed Rulemaking. June 21, 2006, FCC 06-94. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-94A1.pdf (accessed January 31, 2008).

Second Report and Order and Memorandum and Opinion and Order. Communications Assistance for law Enforcement Act and Broadband Access and Services. FCC 06-56, ET Docket No. 04-295, RM-10865. (May 3, 2006), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (accessed January 31, 2008).

Notice of Proposed Rulemaking. 911 Requirements for IP-Enabled Service Providers. FCC 07-108, Docket Nos. 94-102, 05-196, 07-114. June 1, 2007.

Government Documents

The White House, Office of the Press Secretary. "Statement on the Clipper Chip Initiative," April 16, 1993. Reprinted in *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls*. Edited by David Banisar, Electronic Privacy Information Center. Upland, PA: Diane Publishing Co., 1994.

United States Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, 1994.

---. *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.* OTA-CIT-310. 1987.

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.

United States Department of Commerce, National Institute of Standards and Technology. "Memorandum for the Record, March 26, 1990." Reprinted in *Cryptography and Privacy Sourcebook.* Edited by David Banisar and Marc Rotenberg, Computer Professionals for Social Responsibility. Upland, PA: Diane Publishing Co., 1993.

---. *Publication XX: Announcement and Specifications for a Digital Signature Standard (DSS),* August 19, 1991.

---. "Memorandum for the Record, January 31, 1990." Reprinted in *Cryptography and Privacy Sourcebook.* Edited by David Banisar and Marc Rotenberg, Computer Professionals for Social Responsibility. Upland, PA: Diane Publishing Co., 1993.

---. "NIST Announces Voluntary Escrowed Encryption Standard to Promote Secure Telecommunications." http://www.nist.gov/public_affairs/releases/n94-08.htm (accessed February 1, 2008).

---. "Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard." *Federal Register.* Vol. 59. No. 27 (February 9, 1994): 6003.

---. "Public Key Status Report." Reprinted in *1996 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls.*C3. Edited by David Banisar, Electronic Privacy Information Center. Upland, PA: Diane Publishing Co., 1996.

United States General Accounting Office. *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.

United States House of Representatives. "Security and Freedom Through Encryption (SAFE) Act," 105th Cong., 1st sess., 1997, H.R. 695, http://thomas.loc.gov/cgi-bin/query/C?c105:./temp/~c105fX0hvz (accessed January 21, 2008).

---. "Security And Freedom through Encryption (SAFE) Act," 106th Cong., 1st sess., 1999, H.R. 695, http://thomas.loc.gov/cgi-bin/query/F?c106:3:./temp/~mdbsCYnyKP:e0: (accessed January 21, 2008)

---, Committee on Government Operations, Government Information, and Individual Rights Subcommittee. *The Government's Classification of Private Ideas.* 96th Cong., 2nd sess., 1980.

United States House of Representatives, Committee on Government Operations, Subcommittee Computer Security Act of 1987. *Hearings on H.R. 145*. February 25, 26, and March 17, 1987. 100th Cong., 1st sess., 1987, 113-114.

---. *Report on the Computer Security Act of 1987.* House Report 100-153, Part 2. 100th Cong., 1st sess., 26.

United States House of Representatives, Committee on 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 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.,1992.

United States House of Representatives, Committee on the Judiciary, *Report on Telecommunications Carrier Assistance to the Government,* HR 103-827, 103rd Cong., 2nd sess., 1994.

United States Senate. "Comprehensive Counter-Terrorism Act of 1991." 102nd Cong., 1st sess., 1991, S. 266, http://thomas.loc.gov/cgi-bin/query/D?c102:3:./temp/~c102Yj9F8N:: (accessed January 21, 2008).

---. "Encrypted Communications Privacy Act of 1996," 104th Cong., 2nd sess., 1996, S. 1587, http://thomas.loc.gov/cgi-bin/query/D?c104:5:./temp/~mdbsvk1SJt:: (accessed January 21, 2008).

---. "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996," 104th Cong., 2nd sess., 1996, S. 1726, http://thomas.loc.gov/cgi-bin/query/D?c104:3:./temp/~mdbsvGqhA3:: (accessed January 21, 2008).

---. "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997," 105th Cong., 1st sess., 1997, S. 377, http://thomas.loc.gov/cgi-bin/query/F?c105:3:./temp/~mdbsEUhuIG:e0: (accessed January 21, 2008).

---. "Secure Public Networks Act," 105th Cong., 2nd sess., 1998, S. 909, http://thomas.loc.gov/cgi-bin/query/D?c105:1:./temp/~mdbsQJy4Eo:: (access January 21, 2008).

---. "Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999," 106th Cong., 1st sess., 1999, S. 798, http://thomas.loc.gov/cgi-bin/query/D?c106:3:./temp/~mdbsD5PgHl:: (accessed January 21, 2008).

---. "USA Act," 110th Cong., 1st sess., 2007, S. 101, http://thomas.loc.gov/cgi-bin/query/D?c110:5:./temp/~mdbs8aLB2M:: (accessed January 21, 2008).

United States Senate, Committee on the Judiciary, Subcommittee on Technology and the Law, 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., 1994.

United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Hearings on The National Security Agency and Fourth Amendment Rights*, Book 5, October 29 and November 6, 1975, http://www.aarclibrary.org/publib/church/reports/contents.htm. (accessed January 6, 2008).

---, *Intelligence Activities and the Rights of Americans,* Final Report, Book II, April 26, 1976, http://www.aarclibrary.org/publib/church/reports/contents.htm. (accessed January 6, 2008).