UNIVERSITY OF CALGARY

State Autonomy, Corporate Power, and Advanced Electronic Information and Communications Networks: The Digital Signature Standard

by

David Mitchell Trotter

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF ARTS

DEPARTMENT OF POLITICAL SCIENCE

CALGARY, ALBERTA

JUNE, 1999

ABSTRACT

In the latter twentieth century there has been a great deal of rhetoric and activity concerning the development of advanced electronic information and communications networks. The private sector, especially in North America, has assumed the responsibility for developing these networks. This may result in conflict where the wishes of states, markets and corporations collide. This thesis examines the selection and implementation of the Digital Signature Standard (DSS) in the United States. In instituting the DSS, certain executive agencies within the United States government exhibited a high degree of autonomy in the short-term. However, long-term power over public key authentication technologies appears to have been successfully exercised by corporations and markets. This thesis also examines some of the indicators that must be examined in any analysis of state autonomy and corporate power in regard to advanced electronic information and communications networks and suggests further avenues of research.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACF	Advocacy Coalition Framework
ACM	Association of Computing Machinery
AECA	Arms Export Control Act
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AT&T	American Telephone and Telegraph
BXA	Bureau of Export Administration
CBI	Caribbean Basin Initiative
CCITT	International Telegraph and Telephone Consultative Committee
CCL	Commerce Controlled List
CPSR	Computer Professionals for Social Responsibility
CNR	Canadian National Railway
DARPA	Defense Advanced Research Projects Agency
DC	District of Columbia
DES	Data Encryption Standard
DLA	Defense Logistics Agency
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
E-mail	Electronic Mail
EAA	Export Administration Act
EAR	Export Administration Regulations
EDI	Electronic Data Interchange
EES	Escrowed Encryption Standard
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Centre
EU	European Union
FDA	Food and Drug Administration
FIOA	Freedom of Information Act
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GAO	General Accounting Office
GEIS	General Electric Information Services
GII	Global Information Infrastructure
HUD	Department of Housing and Urban Development
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
IEEPA	International Emergency Economic Powers Act
IHAC	Information Highway Advisory Council (Canada)
IMF	International Monetary Fund
IRS	Internal Revenue Service
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations

ITU	International Telecommunication Union
LMI	Logistics Management Institute
MIT	Massachusetts Institute of Technology
MoU	Memorandum of Understanding
MSIE	Microsoft Internet Explorer
NAI	Network Associates Incorporated
NASA	National Aeronautics and Space Administration
NBS	National Bureau of Standards
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSDD	National Security Decision Directive
NSF	National Science Foundation
OECD	Organization for Economic Co-operation and Development
OMG	Object Management Group
OSD	Office of the Secretary of Defense
PGP	Pretty Good Privacy
PKP	Public Key Partners
RSA	Rivest, Shamir and Adleman algorithm
SHS	Secure Hash Standard
TCP/IP	Transmission Control Protocol/Internet Protocol
TWG	Technical Working Group
USDA	United States Department of Agriculture
USMC	United States Marine Corps
USML	United States Munitions List
WWW	World Wide Web

CHAPTER ONE: STATES AND TECHNOLOGY

1.1: Introduction

In the 1990's there has been a great deal of activity in both governments and the private sector related to the development and construction of advanced interactive electronic networks. These networks are referred to by a number of terms, which include "the Information Highway[1]," "Information Superhighway," "National Information Infrastructure (NII)[2]," and "Global Information Infrastructure (GII)."[3] These advanced electronic networks are being used in a number of ways including on-line commerce and banking, accessing government services, information and contact with government officials,[4] educational opportunities, enhancement of the practice of medicine,[5] and countless other applications. Many states have left the development of these information highways to the private sector, although governments may attempt to provide some overall vision and policy coordination for electronic networks. In this situation, some of the policy preferences of states may conflict with those of the corporations who develop the

---

[1] Canada, Information Highway Advisory Council (IHAC), Connection Community Content: The Challenge of the Information Highway (Ottawa: Industry Canada, 1995)

[2] United States, General Accounting Office (GAO), Information Superhighway: An Overview of Technology Challenges (Washington DC.: General Accounting Office, 1995) 10.

[3] Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy, Global Information Infrastructure – Global Information Society (GII-GIS): Policy Requirements, (Paris: OECD, 1997), 5 Feb. 1999 <http://www.oecd.org/dsti/sti/it/infosec/prod/e_97-139.pdf>.

[4] For instance: Patrick B. O'Sullivan, "Computer Networks and Political Participation: Santa Monica's Teledemocracy Project," Journal of Applied Communication Research 23.2 (1995): 93-107.

[5] Kenneth I. Shine, "Impact of Information Technology on Medicine," Technology In Society 18.2 (1996): 117-126.

electronic infrastructure and societal interests which ultimately use these electronic infrastructures. In some instances, the concerns and goals of the state, or elements of the state, may not be given consideration by corporations or societal interests.[6]

This thesis will examine one case study where portions of the American state attempted to implement their policy preferences concerning the development of electronic networks against powerful corporate interests. This case study focuses on the development of the United States government's Digital Signature Standard (DSS). The DSS actually refers to a package of standards, which includes the Digital Signature Algorithm (DSA) which produces the digital signature and a hashing algorithm, which are explained further below. This thesis shows that powerful state actors still have the autonomy to pass and implement their policy preferences, in regard to electronic networks. State autonomy may be defined as:

> ... instances in which state actions are not simply the reflection of the goals and interests of society as expressed through interest groups, elections or classes, but rather when the state has developed interest and goals independently of – though constrained by – society.[7]

However, state actions may not have their intended consequences, since industry and markets have gained overall structural power over how these information and communication infrastructures are constructed and developed. Susan Strange defined structural power as:

---

[6] The development of information infrastructure and national security concerns is one such area. Greg Rattray, "The Emerging Global Information Infrastructure and National Security," Fletcher Forum of World Affairs 21.2 (1997): 81-99.

[7] Christopher McGrory Klyza, and Eric Mlyn, "Privileged Ideas and State Interests: Bombs, Trees, and State Autonomy," Policy Studies Journal 23.2 (1995): 203.

> ... the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic enterprises and (not least) their scientists and other professional people have to operate.[8]

The concept of structural power can also be applied to the entities that make decisions concerning the standards used in the construction and development of global electronic networks and whether these entities are predominately public or private. In addition, this thesis will attempt to show that state and corporate relations do not automatically fall into "us versus them" relationships. Reality is actually more complex, since some corporate actors may support state actions while other parts of the state may side with corporate actors against other parts of the state.

The first chapter of this thesis examines the selection of the case study, background information on the "information highway" and "digital signatures," academic study of the state, how states are changing and, the interaction of states and technology. In addition, chapter One also discusses a complementary micro-level societal perspective that examines the belief structures of the participants involved in the DSS. Chapter Two deals with perceived instances of state control over, and involvement in, cryptography policy, the development of the DSS and the public comments regarding the DSS and the long-term results. The third chapter briefly deals with events after the DSS and focuses on the Escrowed Encryption Standard (EES) and the development of the Advanced Encryption Standard (AES). In addition, United States export controls on cryptographic products will be briefly

---

[8] Susan Strange, States and Markets 2nd ed. (London: Pinter, 1994) 24-25.

examined. Chapter Four contains the conclusion, which draws lessons for the application of existing theories concerning the state and politics to advanced electronic information and communication networks and suggestions for further research in this area.

One issue that needs to be clarified before proceeding is the issue this thesis will analyze. This thesis examines the conflict between executive agencies and corporations in setting a United States government standard for digital signatures. This issue attracted the attention of other governmental agencies, corporations and individuals since the proposed standard could have had impacts on the private sector. This conflict involves concerns about authentication and communications security. A number of other publications have dealt with privacy issues related to the collection and disclosure of personal information contained in computer networks and databases.[9] Authentication, security and privacy are not totally distinct issues, since there is a great deal of overlap and inter-relatedness among them. Technologies such as cryptography can be used to protect privacy while others, such as computer databases, video surveillance, wiretaps and key-recovery technologies may be used to compromise privacy. Cryptography policy does not appear to have been studied in depth by many political scientists and thus it is hoped that this under-explored policy area can provide some insights about the power and autonomy of states and corporations in an era of advanced electronic networks.

---

[9] For instance: Philip E. Agre, and Marc Rotenburg, eds. Technology and Privacy: The New Landscape (Cambridge: MIT Press, 1997)

At first glance the United States may appear to be a poor choice for a case study since the United States is often portrayed as having a relatively weak state. The United States does not have a centralized and powerful bureaucratic state, unlike many European and Asian countries. In addition, other factors such as federalism and the separation of powers also reduce the power and autonomy of the American state. A well known study, which examined the differing power of domestic state structures, was conducted by Peter Katzenstein. Katzenstein's analysis of the foreign economic policies of France and the United States demonstrated that domestic structures play a significant role in foreign economic policy. According to Katzenstein, domestic structures reflect different measures of state and society. France has a strong state and a weak society. The inverse is true of the United States. In France, the state was actively involved in foreign commercial, financial and energy policy. In contrast, private interests in the United States determined foreign economic policy in the commercial, financial and energy sectors for the most part.[10] One author makes the distinction between the "administration" which is comprised of the executive agencies and the president and the "state" proper, which includes all political institutions, including sub-national governments and local institutions, and the relations between them.[11] However, certain provisions can be made for some areas of the state to be more autonomous than others:

---

[10] Peter J. Katzenstein, "International relations and domestic structures: Foreign economic policies of advanced industrial states," International Organization 30.1 (1976): 1-45.

[11] Andrew J. Stritch, "State Autonomy and Societal Pressure: The Steel Industry and U.S. Import Policy," Administration and Society 23.3 (1991): 291.

> ...On any issue, if comparatively autonomous state fragments prevail over less autonomous ones in the policy-making process, then we can still regard the state, in aggregate, as having a high degree of autonomy on that issue. ...[12]

Academic examination has found that parts of the American state can occasionally act in an autonomous manner. Stephen Krasner in his book, *Defending the National Interest*, examined American policy regarding raw materials and whether policy related to raw materials was susceptible to manipulation by corporate interests. He shows that some parts of the American state were able to act autonomously since they were "insulated" from Congressional involvement.[13] Another work by Theda Skocpol and Kenneth Finegold dealing with agricultural policy under the "New Deal" claims that the U.S. Department of Agriculture (USDA) was able to exercise considerable levels of autonomy. This was due to the considerable amount of expertise that the USDA exercised.[14] Another researcher also noticed that the American state was successful in resisting demands from powerful business and labor interests in the steel industry. In this instance, the American state was successful in resisting demands for protectionist measures on

---

[12] Stritch 296.

[13] Stephen D. Krasner, Defending the National Interest: Raw Materials Investments and U.S. Foreign Policy (Princeton: Princeton UP, 1978) cited in Theda Skocpol, "Bringing the State Back In: Strategies of Analysis in Current Research," Bringing the State Back In, eds. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambrige UP, 1985) 12-13.

[14] Theda Skocpol, and Kenneth Finegold, "State Capacity and Economic Intervention in the Early New Deal," Political Science Quarterly 97.2 (1982): 255-278. cited in Theda Skocpol, "Bringing the State Back In: Strategies of Anaylsis in Current Research," Bringing the State Back In, eds. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambrige UP, 1985) 13.

foreign steel imports.[15] The policy process concerning encryption standards has been relatively "insulated" to use Krasner's terminology. The governmental agencies most directly involved are divisions of executive agencies, such as the National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards (NBS)). In addition, the National Security Agency (NSA), part of the Department of Defense, has also had, or is alleged to have had, significant involvement in determining American encryption policy as will be demonstrated later in the thesis. In addition, policy making in areas that concern national security is usually more secretive than other domestic policy making.[16] This could result in more "insularity" where national security interests are involved.

The policy process surrounding the creation of a Federal Information Processing Standard (FIPS) is another reason for the selection of the United States as a country for a case study. The enactment of the Brooks Act in the 1960's, acted as a guide for government purchases of information technology. In order to achieve the goals of the legislation, Federal Information Processing Standards were instituted.[17] The process by which a FIPS gets adopted is dominated by executive agencies and is rather atypical of American policy making when contrasted with other areas such as social policy, economic policy and defense policy. In these areas, there are usually on-going dialogues with

---

[15] Stritch 288-309.

[16] Ronald J. Stupack, and Thomas C. Hone, "National Security and Domestic Policy Making: The Similarities and the Critical Differences," International Journal of Public Administration 15.7 (1992): 1444.

Congress and the Judiciary. Congressional and judicial involvement in the adoption of a FIPS is relatively non-existent. The FIPS approved by the NIST must ultimately be endorsed by the Secretary of Commerce. Adherence to the FIPS is mandatory for federal government agencies, although federal agencies may "opt-out" of a FIPS. The Federal Information Processing Standards have come to have larger implications for organizations outside the United States federal government. Due to the quantity of government procurement and other factors, the United States government standards are often adopted by the private sector.[18] Standards are very necessary for the development of communication networks since they provide for a common method of achieving some end, such as interconnection.[19] Governments can also use standards as policy instruments designed to achieve government or state ends as demonstrated by the DSS and later EES.

The DSS appears to be treated in many accounts as a small skirmish in cryptography policy battles in the United States. Many commentaries only devote a few pages to it. An argument can be made that an examination of the later and more controversial Escrowed Encryption Standard (EES) and the associated

---

[17] Whitfield Diffie, and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (Cambridge: MIT Press, 1998) 58.

[18] Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution," University of Pennsylvania Law Review 143.3 (1995): 764-766.; Karen E. Gegner and Stacy B. Veeder, "Standards Setting and Federal Information Policy: The Escrowed Encryption Standard (EES)," Government Information Quarterly 11.4 (1994): 410-411.

[19] Richard Hawkins, "Standards for Communication Technologies: Negotiating Institutional Biases in Network Design," Communication by Design: The Politics of Information and Communication Technologies, eds. Robin Mansel, and Roger Silverstone (Oxford: Oxford UP, 1996) 157-159.

"clipper chip," would present a better case study of state autonomy and power or the lack thereof. The DSS was chosen for a number of reasons.

First, a number of government agencies, corporations and industry associations, members of the academic community and individuals submitted comments in response to the proposed DSS. The government agencies that submitted comments included the Departments of Commerce, Defense, Energy and the Treasury. Some of the corporations that submitted comments in regard to the DSS included Digital Equipment Corporation, International Business Machines Corporation (IBM), Motorola, Microsoft Corporation, Sun Microsystems, and Xerox. These are some of the leading firms responsible for developing electronic infrastructure and applications, and as such, their opinions of the DSS would be critical in assessing its usefulness in the development of advanced electronic networks. The comments received regarding the EES had many more individual responses, but lacked the number of corporate responses that characterized the DSS. [20] However, both the DSS and the ESS demonstrate the limited ability of parts of the American state to fully implement their policy preferences. In addition, there was an international aspect to the responses to the DSS, since some of the firms that submitted comments, such as Northern Telecom and Bull SA, were foreign firms.

---

[20] The controversy surrounding the DSS occurred before the widespread adoption of the Internet. Widespread electronic public discourse would have been limited at this time. In addition, the subject of standards for digital signatures would have only been a salient issue for a small number of persons.

Another concern is that the United States government does not consider digital signature technology to be a threat, unlike other cryptographic technologies. As Diffie and Landau have noticed, the United States government only considers cryptographic applications as dangerous when they are used to conceal the content of messages.[21] However, despite the non-threatening nature of digital signature technology, there appears to have been a great deal of government involvement in the development of the DSS and its adoption as a United States government standard.

Another reason for the selection of the DSS as a case study is that it appears to be relatively free of "rights rhetoric," unlike other cryptography battles, which can involve rights claims.[22] Rights rhetoric refers to claims made on the basis of the rights enumerated in entrenched constitutional documents, such as the United States Bill of Rights. The relative lack of rights rhetoric makes the DSS more useful for examining state autonomy vis-à-vis industry and markets, since this issue is not obscured by rights claims made against government laws and/or actions based on the perceived violation of inalienable individual rights. The submission from the Computer Professionals for Social Responsibility (CPSR), in

---

[21] Diffie and Landau 12. Note: Intelligence agencies also have an interest in the amount and nature of the communications traffic between the origin and destination, as well as the content of messages. Diffie and Landau 92.

[22] Many authors have examined rights issues found in the encryption policy, either in whole or part. In regards to constitutional rights and encryption see: Froomkin 709-897.; Kristine M. Nelson, "The Clipper Initiative: Fact or Fiction in Future Encryption Policy," Hamline Journal of Public Law and Policy 16.1 (1994): 291-311.

regard to the proposed DSS does mention "a right to disclosure."[23] However, this appears to refer to a matter of administrative law concerning access to government information, rather than any type of constitutional rights claim.

1.2: What is the Information Highway?

Most visions of the "information highway" involve the connection and integration of traditionally distinct communications networks such as the telephone network, cable systems and wireless systems including cellular and satellite services into one large super- electronic network. The Internet, by itself, is not the "information highway," although the various computer networks and protocols that comprise the "Internet" are also included within the "information highway." The Internet refers to computer networks that use the Transmission Control Protocol/Internet Protocol (TCP/IP). These networks include the World Wide Web (WWW), Telnet, File Transfer Protocol (FTP), electronic mail (E-mail), Usenet news groups and others. These advanced electronic networks consist of more than just the physical infrastructure such as wires, fiber optic cable, telephone exchanges, cable trunk lines, satellite dishes and other means of transmission. These electronic networks are also comprised of other hardware, software, applications, information, and services. In addition, the administration and maintenance mechanisms are also included in the definition of the "information highway." Integration of these networks has been made possible by

[23] Marc Rotenberg and David Sobel, letter to Director, Computer Systems Laboratory, 24 Oct. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

digitalization.[24] In some cases these electronic networks work together to relay communications traffic. One such example is Internet telephony. Internet telephony involves using the leased telephone/cable lines used for the Internet to carry conventional telecommunications traffic. Some telecommunications operators already offer Internet telephony services.[25] However, there is a great deal of controversy regarding other elements of technological convergence, such as that between the WWW and television. Considerable uncertainty exists on how, or if, the WWW and television will be integrated. Many questions regarding business models, support mechanisms, and the content to be provided have yet to be resolved.[26] However, despite this uncertainty, some Internet television and radio broadcasting operations have emerged.[27]

There are many policy challenges posed by the development of the information highway, some of which have been discussed by Jeremy Mitchell. One of the policy challenges results from the integration of the various networks that comprise advanced electronic interactive networks. These networks have been, and remain, covered by individual policy areas such as telecommunications,

---

[24] United States, General Accounting Office (GAO), Information Superhighway: An Overview of Technology Challenges, 10-17.

[25] Michael Tyler, Briefing Report on Transforming Economic Relationships in International Telecommunications (Geneva: ITU, 1998) 101; AT&T Expands Availability of Internet Telephony Service, AT&T, 5 Nov. 1998, 5 Mar. 1999 <http://www.att.com/press/1198/981105.csb.html>.

[26] James Ledbetter, "TV-Web Convergence; Now? Ever?" The Industry Standard: The Newsletter of the Internet Economy 27 Jan. 1999, 29 Jan. 1999 <http://www.thestandard.net/articles/article_print/0,1454,3298,00.html>.

[27] Examples of these services include DENtv and DENradio. Welcome to DENtv.com, Interactive Netcasting Systems Inc., 21 March 1999 <http://www.dentv.com/index.shtml>.; Welcome to DENradio.com, Interactive Netcasting Systems Inc., 21 March 1999 <http://www.denradio.com/index.shtml>.

broadcasting and computing and each of these areas have distinct policy inheritances. The distinction between these areas is increasingly being called into question. The policies and practices adopted in one area may conflict with the policies and practices in another area. One area where this is apparent is universal service. In some countries, broadcasting is readily available to a majority of the population, although there may be a tax imposed on recipients. However, in telecommunications the intention has usually been to provide services at a reasonable cost. Other contentious policy issues surrounding these advanced electronic networks involve content issues such as indecent and dangerous material and privacy issues.[28] Other policy challenges arising from electronic networks, especially the Internet, are due to technological factors, which challenge national regulatory frameworks. Information in electronic form can be passed from country to country without regard for national regulations.[29]

1.3: Cryptography and Digital Signatures

Many communication networks, and especially the Internet, do not use secure channels for communication. This means that messages, such as electronic mail (E-mail), can be monitored, read and possibly changed as they pass from one computer to another. Sensitive information such as personal information and credit card numbers are in jeopardy of being used by others with

---

[28] Jeremy Mitchell, "Convergent Communications, Fragmented Regulation and Consumer Needs," Telecom Reform: Principles, Policies and Regulatory Practices, ed. William H. Melody (Lyngby: Technical University of Denmark, 1997) 441-451.

[29] For a more detailed account of technological challenges see: Andy Johnson-Laird, "The Anatomy of the Internet Meets the Body of the Law," University of Dayton Law Review 22.3 (1997): 467-509.

malicious intent. Since identity cannot be easily verified in cyberspace, a person could send messages claiming to be from another person.[30] This practice is colloquially known as "spoofing." Cryptography is one method that can be used to secure electronic communications. Digital signatures are an application of cryptography, and public key cryptography in particular. The term "digital signature" is actually misleading since the term suggests that the "signature" is a digitized copy of a hand written signature. Digital signatures as applications of cryptography involve complex mathematical operations and as such are more difficult to forge.

Cryptographic systems and the mathematical algorithms on which they are based can be broadly classified as either symmetric or asymmetric (public key cryptography). A symmetric cryptographic system uses the same key to encrypt and decrypt data. Professors Whitfield Diffie and Martin E. Hellman laid the theoretical foundations for public key or asymmetric cryptography in the late 1970's.[31] However, Professors Ron Rivest, Adi Shamir and Leonard Adleman implemented the theory into practice by developing the public key algorithm, RSA, which can be used for both encryption and producing digital signatures.[32] Public key cryptography uses two related but distinct keys, the public key and the private key. The public key is used to encrypt data and is made available to others who

---

[30] The anonymity offered in "cyberspace" is somewhat overstated. It is possible to gather personal information on the Internet through technical means.

[31] Whitfield Diffie, and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory IT22.6 (1976): 644-654.

wish to send encrypted messages to the owner of the public key. The private key is kept secret since it is used to decrypt data encrypted with the corresponding public key. The private key is protected by a passphrase. The key pair is constructed in such a fashion that it is difficult to determine the private key from the public key. Both cryptographic systems, symmetric and asymmetric, can be used to generate digital signatures. In a symmetric system, trusted third parties or "arbitrators," are used to "digitally sign" a message. In a public key system, the private key can be used to generate a digital signature, which can be verified by the corresponding public key. When a message is digitally signed only part of the actual message is signed with the private key. A one-way hashing function is used to compress the message being signed into a "hash," which is transmitted with the message. This hash is called a "digest." The digest is then encrypted or "signed" with the owner's private key. The public key is used to verify the message. If the verification function is successful, the recipient of the message can be reasonably assured that the sender is whom he or she claims to be and that the message has not been altered. In addition, a time stamp may be added to digital signatures in order to increase their level of security by indicating when the electronic document was digitally signed.[33]

---

[32] "RSA Labs FAQ – What is RSA?" RSA Laboratories, FAQ 4.0, RSA Data Security Inc., 3 March 1999 <http://www.rsa.com/rsalabs/faq/html/3-1-1.html>.

[33] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd ed. (Toronto: John Wiley and Sons, 1996) 34-41.; Philip R. Zimmerman, "Cryptography for the Internet," Scientific American Oct. 1998: 112-113.

Digital signatures perform three functions. The first function is to provide proof of origin. Digital signatures can be employed to verify a person's identity, since the correspondent, ideally, should be the only person to know the passpharse to the private key. The second function performed by digital signatures is to verify the integrity of the message so that the recipient can be reasonably assured that the message was not altered or tampered with while in transit. Since the "hash" of the message is based on the original composition of the message, any changes, no matter how minor will change the hash and as a result, the public key will not verify the message. One application of a digital signature in this regard is to protect the integrity of software that is sent over electronic networks. The company or individual sending the software over the network may digitally sign the software. If the software has been tampered with the recipient will be aware of this. Digital signatures in this instance would act as an electronic form of the wrapping found on software packages in stores. Microsoft Corporation uses a system called "Authenticode" which employs digital signature technology in order to ensure the integrity of software and computer code available for downloading over the Internet.[34] A third function of a digital signature is non-repudiation. In this case, a sender cannot deny sending a message.[35] This would prove especially useful in holding people accountable for statements made over electronic networks. The usefulness of digital signatures in this regard was recently

---

[34] Introduction to Code Signing, Microsoft Corporation, 29 Oct. 1998 <http://www.microsoft.com/workshop/security/authcode/intro_authenticode.htm>.

[35] Michael J. Ganley," Digital Signatures and Their Uses," Computers and Security 13.5 (1994): 385.

demonstrated in the trial and conviction of Carl Johnson who posted threats against government personnel and a business leader on an electronic mailing list. The messages included Johnson's digital signature, which allowed prosecutors to establish that Johnson posted the threatening messages on the mailing list.[36] In addition, other persons have suggested that another use for digital signatures is to obtain commitment on electronic documents, such as contracts for goods or services.[37]

However, a problem arises since anyone can create a pair of public-private keys and then impersonate another individual. The impersonator could then give his or her public key as the public key of the intended recipient. This problem can be solved with a certification authority. A certification authority is a trusted third party, which binds a public key to a particular person, the subscriber, by a digital certificate. Certification authorities can be specialized private companies, branches of existing companies or even government agencies. The digital certificate issued by the certification authority contains the private key of the certification authority itself. The validity of the certificate is based on the certification authority's private key. The certification authority's public key is made available to anyone who needs to verify its private key and may even be found in computer programs, such as web browsers. If a subscriber's private key is

---

[36] Chris Stamper, "Guilty Verdict for Cypherpunk," Wired News 20 Apr. 1999 <http://www.wired.com/news/print_version/politics/story/19239.html?wnpg=all>.

[37] A. Herzberg, and D. Naor, "Surf'N'Sign: Client Signatures on Web Documents," IBM Systems Journal 37.1 (1998): 61-71.

compromised the certification authority is notified and the certificate is placed on a list of revoked certificates to inform others that the digital signature has been compromised.[38]

Digital signature technology has attracted a great deal of attention lately in legal and policy circles. Many of the state governments in the United States and other states in the world are in the process of developing the legal and policy frameworks for the use of digital signatures.[39] In the early stage of development some of these policies and laws may have problems. One author has noticed that the Utah Digital Signature Act has problems in regard to liability and evidence for persons and organizations involved in a public key infrastructure.[40]

As mentioned earlier, this thesis examines the autonomy and structural power that the American state, and states in general, have to influence the design and development of advanced electronic networks. The competition between technologies which are supported by a state, and those supported by industry, gives an indication as to whether states or corporations exercise power over the development of advanced electronic networks. However, in order to examine state autonomy in this policy area, an examination of the theoretical literature on how states and state autonomy have been studied is required. The theoretical literature

---

[38] Warwick Ford, "Digital Certificates," Scientific American Oct. 1998: 108.

[39] Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy, Group of Experts on Information security and Privacy, Inventory of Approaches to Authentication and Certification in a Global Networked Society, 16 Oct. 1998 <http://www.ottawaoecdconference.org/english/announcements/reg3r3e.pdf>.

[40] C. Bradford Biddle, "Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure," San Diego Law Review 33.3 (1996): 1143-1193.

is intended to provide background on how, and under what circumstances, states have exercised autonomy.

1.4: The State as an Object of Academic Investigation

Theda Skocpol in the article, "*Bringing the State Back In*" published in the mid-1980's, noticed that the state had re-emerged as an object of academic investigation in explaining political phenomena. The statist perspective proceeds from the assumption that states and their associated apparatus have impacts on poiitics. In the post World War II era, especially in the 1950's and 1960's, society based explanations of political behavior were popular. There was also a strong historical momentum for focusing on societies rather than states. Factors such as industrialization and democratic agitation in the 18th and 19th century contributed to this. The dominance of British and then of American social science also reinforced the focus on society in explanations of political phenomena. The society-based models assumed that politics arose in society and that states and the associated institutional apparatus only acted as a catalyst for political phenomena. Using this analogy, societal interests were the reactants, which produced politics. However society-based models were shown to be deficient when applied to many situations, such as explaining certain political phenomena in Western Europe. During this time, the state had not been completely abandoned as an object of analysis. Neo-Marxists had continued to focus on states in their analyses. However, in neo-Marxist thought, the state was considered in the context of class conflict. The state was associated with the capitalist class, and as such was not completely

independent.[41] In addition, neo-Marxist theories were applied to all states, irrespective of institutional structures. This meant that that the effects of different institutional configurations could not be examined. Continental European and especially German social science also had not completely abandoned the state.[42]

Stephen D. Krasner, like Skocpol, also notices the re-emergence of the state as a subject of research in the social sciences. He compares some recent work focusing on states to the dominant behavioural perspective used in social and political science research after World War II. He notices five differences between the behavioural and statist perspectives in research that he reviews. The first involves different notions concerning politics. In statist research, the focus is on the maintenance of security and law and order. In the behavioural view, the focus is on the apportionment of public and political goods. Second, statist research considers the state as a political actor in and of itself, while behavioural approaches do not. Third, statist research assumes that individuals can be constrained by institutional arrangements. The institutional arrangements can determine perspectives and the amount of political resources available to a person. Fourth, statist views are more aware of the role of historical factors than the

---

[41] One Canadian neo-Marxist scholar, Leo Panitch, has noticed this. According to Panitch, the state has to act independently of the capitalist or propertied class in order to ensure the long-term survival of the capitalist system. If the capitalist classes were directly in charge, they would choose short-term gain at the expense of the long-term survival of the capitalist system. Leo Panitch, "The Role and Nature of the Canadian State," The Canadian State: Political Economy and Political Power, ed. Leo Panitch (Toronto: UT Press, 1987) 4.

[42] Skocpol 4-7.

behavioural perspective. Fifth, the statist perspective is better at highlighting potential political conflict than the behavioural perspective.[43]

Theda Skocpol in examining state-centered research in *Bringing the State Back In* notices two ways in which states have been examined. The first method has involved examining states in term of their autonomy to implement their favored policies.[44] A number of factors are required for states to achieve their policy preferences. Some basic factors of state capacity include *de facto* control over a territory, bureaucrats with significant levels of expertise, and financial resources. In regards to financial resources, a state's ability to both tax and borrow funds and the discretion to spend funds as it sees fit are key elements of state power. State capacity is not uniform and may differ over a number of policy areas.[45]

Like Skocpol, Krasner has also noticed this particular research orientation. Krasner cites Eric Nordlinger's book, *On the Autonomy of the Democratic State*, in this regard. In this book, Nordlinger uses a typology of state autonomy based on three types. In Type III state autonomy, the preferences of state and societal actors are the same, thus state preferences are uncontested. In Type II state autonomy, states change the preferences of societal actors to conform to those of the state. Various means may be used to accomplish this, such as resource transfers to like-minded societal actors and resource removals from actors whose

---

[43] Stephen D. Krasner, "Approaches to the State: Alternative Conceptions and Historical Dynamics," Comparative Politics 16.2 (1984): 224-225.

[44] Skocpol 9-14.

[45] Skocpol 16-18.

preferences are contrary to those of the state. Type I state autonomy occurs when state preferences triumph over opposing societal preferences. In Type I autonomy, states may either remove or transfer resources to like-minded or opposed groups or conceal decision-making procedures.[46]

The second perspective discussed by Skocpol is called "Tocquevillian." In this perspective the organization of state institutions and actions influence a number of factors within the state. The factors include the thoughts and beliefs concerning politics, the mobilization of certain groups and interests, and the issues that are dealt with by state organizations.[47]

Krasner, in his review of state-oriented research, also notices another perspective used by researchers who undertake studies of the state and changes to the institutional structure of the state. According to Krasner, states may be studied as conduits through which external and internal forces manifest themselves. This perspective examines how states and their institutions respond to these forces and then how states and their institutions can exercise reciprocal influence on the broader environment. Two patterns can emerge where states and the broader environment are at odds. The first is termed "public stasis and private dynamism." In this pattern, the forces for change are internal. One example of this perspective involves the study of industrialization and its effects on the state and its institutions. Industrialization had resulted in the emergence of centralized

---

[46] Eric Nordlinger, On the Autonomy of the Democratic State (Cambridge: Cambridge UP, 1981) cited in Stephen D. Krasner, "Approaches to the State: Alternative Conceptions and Historical Dynamics," Comparative Politics 16.2 (1984): 231.

[47] Skocpol 24.

bureaucracies in many countries except the United States. In the United States, the political institutions were not conducive to the strengthening of the state. The second pattern is termed "state demands and societal resistance." In this perspective, the impetus for change is external. One study cited by Krasner, deals with the effects of military threats on states. The threat results in the expansion of bureaucracies, which leads to higher levels of taxation, which leads to tension with society.[48]

States are not the only actors in international politics. The latter part of the twentieth century has witnessed the development of powerful transnational corporations, interest groups, and even transnational criminal organizations that challenge the power of states.[49] Theories that examine the state's role in policy making must deal with the emergence of these powerful new forces. Scott Turner offers a critique of the liberal framework in which the relationship between states and corporations is portrayed as a "zero-sum game," where states lose power to corporations. Turner believes that the relationship between states and corporations is more nuanced than commonly believed and suggests a new framework for analysis that considers this fact. One of his assumptions is that "the relationship between states and corporations can be both adversarial and

---

[48] Krasner 234-239.

[49] Susan Strange, The Retreat of the State: The Diffusion of Power in the World Economy (Cambridge: Cambridge University Press, 1996)

cooperative."[50] Cooperation may also result in diminished state autonomy, even though state power may be intact. State power may be used to enhance the power of corporations. Turner illustrates this tendency with examples of U.S. policy. One such case involved the Caribbean Basin Initiative (CBI). One object of the CBI was promoting economic development in the Caribbean. The policy instruments used were loans and foreign direct investment. U.S. based transnational corporations benefited from the program since it made importing and exporting their goods to Caribbean countries easier and less costly. The program limited the autonomy of participating countries since this program dictated their trade policy. Corporations require state power in order to implement their policy preferences. However, since the state is implementing corporate policy preferences, it is limited in its ability to protect groups that are negatively affected by these decisions.[51]

One pair of authors has argued that the ideas underlying the interests of the state are a crucial part of state autonomy. In cases where states have exhibited autonomous behavior for more than twenty-five years, the source of state autonomy is an idea that has been adopted by technocrats. According to the authors, this idea becomes "privileged."[52] Ideas are important since they "can in

---

[50] Scott Turner, "Transnational Corporations and the Question of Sovereignty: An Alternative Theoretical Framework For the Information Age," Southeastern Political Review 25.2 (1997): 304

[51] Turner 310-314.

[52] Klyza and Mlyn 203-204.

some cases influence policy by influencing the strength of policy options and the nature of debate over them."[53]

The notion that the state is in decline is the subject of considerable debate in political science in the late twentieth century. However, many scholars have noticed that the nature of state power and its position vis-à-vis other actors is currently undergoing change. The next section examines some of the literature concerning whether or not states have lost autonomy and power.

1.5: The Changing Nature of the State

In the latter part of the twentieth century, there are a number of differing opinions regarding state autonomy and the decline of the state. Uncertainty exists as to whether the state is gaining power or losing power or even whether the state is in decline.

Susan Strange believes that state authority has diffused to other institutions and organizations. This authority involves powers once exercised by states that have come to be exercised by other actors. State authority has diffused to some international organizations and groups such the European Union (EU), the International Monetary Fund (IMF) and, Amnesty International. In some instances state authority has diffused to sub-national governments. State authority has also diffused sideways to other organizations such as transnational corporations. Corporations and other entities now are exercising power with states in areas such as economic development.[54] However, in another work Strange does concede

---

[53] Klyza and Mlyn 205.

[54] Susan Strange, "The Defective State," Daedalus 124.2 (1995): 63, 67-69.

that state authority may be diffusing downward and sideways more than upward.[55] Strange attributes the loss of state power to three structural factors, technology, markets, and politics. States have lost control over the development of technology, while markets have assumed some state responsibilities. Strange also argues that politics is not limited to state organizations, but is an activity practiced by many other non-state organizations.[56]

Michael Mann is one commentator who is critical of the claim that states are in decline. He assesses four forces that could conceivably threaten the viability of the nation-state. The first force is global capitalism. Global capitalism and its associated neo-liberalism are believed to be transnational in scope and beyond the scope of effective government regulation. However, capitalism is not necessarily global since it is limited primarily to Europe, North America and parts of Asia. In addition, states are required to maintain optional conditions for global markets. States are also involved in and influence the world economy through international organizations such as the International Monetary Fund (IMF). The second force is environmental problems. The environment is perceived as a shared concern or a "tragedy of the commons" type problem, which may involve more than one state. However, even though problems are internationalized, state action is required to deal with these problems. The third force is identity politics. Identity politics has been facilitated by new information and communications technologies, such as the Internet, which allow for more interactions between local and transnational

---

[55] Susan Strange, The Retreat of the State 185-186.

[56] Susan Strange, The Retreat of the State 42.

identities, such as environmentalism, pacifism, and feminism. New technologies allow these identities to form networks that are transnational, thus bypassing states. It is believed that these new transnational identities may command more support than the traditional nation state. However, state action is required to protect and enhance the rights of these groups. The fourth force is termed "post nuclear geo-politics" or "hard geo-politics." According to post-nuclear geopolitics, the destructive power of modern weapons has undermined the state's security provision role since they cannot be used without inflicting significant damage. However, this applies to some states more than others, since "hard geo-politics" continues to be played between countries such as India and Pakistan.[57]

Peter Evans is one researcher who has examined the possibility of the state being "eclipsed" or overwhelmed by other non-state institutions and forces. He believes that there is only a remote chance of states being eclipsed by other forces. One force that could lead to the eclipse of the state is the new global political economy. This refers to globalization, which involves an increase in trade. According to Evans, this increase in trade does not signify either the decline or the eclipse of the state. The presence of a large and powerful state may have economic advantages. Evans also discusses two factors that are independent of globalization, but also indicate that the state is in decline. These factors are neo-

[57] Michael Mann, "Has globalization ended the rise and rise of the nation-state?" Review of International Political Economy 4.3 (1997): 472-496.

classical economics and new conceptions of civil society.[58] However, contrary to expectations of limited state involvement in the economy, a strong intellectual property regime upheld by states is required due to the increasing trend toward the commodification of ideas. The state is also seen by many to be a hindrance or threat to "civil society." The belief is that many political and social problems are the result of too much state interference in the lives of ordinary persons. There is a belief that a better quality of life would result from less state interference. However, Evans notices some research that has shown that there is an interdependent relationship between society and state.[59]

Peter F. Drucker is another researcher who is not convinced that states are in decline. He notices that ideas about the decline of the state are not new. Political theorists such as Karl Marx and others discussed this possibility. However, the state is changing especially in areas of fiscal and monetary policy, foreign economic policy, policy related to multinational business, and potentially military policy. The global currency market has created a pool of "world money" that exists only in electronic form, but has significant power. This pool of world money is extremely volatile and if states do not adopt certain policy measures, such as balanced budgets, this can have significant negative repercussions since the expectations of those who control the "world money" may not be satisfied.

---

[58] Evans does not elaborate on what the term civil society actually means. However, his description is consistent with neo-conservatism advocated by political leaders such as Ronald Reagan and Margaret Thatcher.

[59] Peter Evans, "The Eclipse of the State? Reflections on Stateness in an Era of Globalization," World Politics 50.1 (1997): 62-87.

Failure to conform to the expectations of those who control the "world money" could result in capital outflow, triggering the devaluation of a country's currency and financial hardship.[60] In this new environment, international economic policy will have to be more concerned with investment instead of commodities, since investment can stimulate trade. In terms of international business, many companies are in the process of transforming from multinational corporations to transnational corporations. Drucker even believes that the concept of "total war" characteristic of past warfare may be incompatible with global production, in that potential belligerents would lack some of the materials and parts required to effectively support an armed conflict.[61] However, this may not apply to countries that are outside, or marginal to, the world economy (i.e. Yugoslavia (Serbia)).

Conventional wisdom in regard to globalized markets is that state regulation creates unnecessary barriers, and should be reduced as far as possible. One author who examined regulation governing national stock exchanges in Germany noticed that state involvement is actually necessary in internationalized stock markets. In the case study, the German government was actually forced to adopt stricter regulations on stock exchanges in regards to insider trading and investor protection than the self-regulation previously practiced by German stock markets.[62]

---

[60] This was demonstrated by the Asian economic crisis. The government of Thailand failed to take action to prop up the value of their currency. This resulted in a devaluation of the Thai currency, which spread to other Asian currencies. One result of the crisis was capital flight from the Southeast Asian region.

[61] Peter F. Drucker, "The Global Economy and the Nation-State," Foreign Affairs 76.5 (1997): 159-171.

[62] Susanne Lütz, "The revival of the nation-state? Stock exchange regulation in an era of globalized financial markets," Journal of European Public Policy 5:1 (1998): 153-168.

In regard to telecommunications, authors have made differing assessments of state autonomy and power in this area. Susan Strange believes that telecommunications is one area where the decline of the state is most noticeable. Technological and economic factors have forced many states to privatize state-controlled telecommunications operators and liberalize telecommunications markets.[63] Derrick Cogburn's examination of telecommunications reform in South Africa, noticed that the South African state exercised a great deal of autonomy over societal interests, both business and labor, in devising that nation's telecommunications policy.[64]

Up to this point, certain communication and information technologies and the changing nature of state power have been discussed. In order to fully explore the issue of state autonomy, corporate power and advanced electronic networks it is necessary to explore the relationship between states and technology. States can be seen as the victims of technological change since they may lose the ability to regulate certain aspects of advanced electronic networks. However, this discussion proceeds from the premise that the selection of technologies is an inherently political process. States do not passively react to information and communication technologies, but may attempt to influence the development, design, and use of certain technologies.

---

[63] Strange, The Retreat of the State 100.

[64] Derrick L. Cogburn, "Globalization and State Autonomy in the Information Age: Telecommunications Sector Restructuring in South Africa," Journal of International Affairs 51.2 (1998): 583-604.

1.6: The Relationship Between States and Technology

One author, Klaus Lenk, has noticed that new information and communications technologies may have undermined the exercise of state power in one important area, the ability to police society. According to Lenk, the ability to police within a defined territory is one of the basic functions of the state. New information and communications technologies allow criminal activities to be planned, mobilized and executed from a variety of different locations. Thus, the destructive effects of criminal activity may be far removed from the area in which they were originally planned. Criminal activity in this context is globalized. This contrasts with the limited ability of law enforcement to coordinate effective responses to globalized crime due to preoccupations with national sovereignty and the integrity of national borders.[65] However, states may react by developing and using new or existing technologies to counter the use of information technology by criminals.

One usually forgotten fact is that the selection and use of technologies is an inherently political process. Jos Huigen in his examination of two Electronic Data Interchange (EDI) projects in the public sector in the Netherlands proceeds from two assumptions. The first is that ambiguity and uncertainties are found in these projects. The second is that there are political considerations in these projects. The first of Huigen's case studies was a planned national population database, which was to be used for policy making. The second of Huigen's case studies

[65] Klaus Lenk, "The challenge of cyberspatial forms of human interaction to territorial governance and policing," The Governance of Cyberspace: Politics Technology and Global Restructuring, ed. Brian D. Loader (New York: Routledge, 1997) 126-135.

involved an EDI project in Rotterdam harbour. In both projects, political considerations were key to the design and development of these electronic projects.[66]

State involvement in selecting technologies for political purposes has not been limited to the twentieth century or to the United States alone. One article that examines the founding of the Canadian National Railway (CNR) illustrates that the Canadian government created the CNR in order to increase state power and control in Canada over economic development.[67] The technologies employed in this situation were that of the Crown Corporation and railways. The case of the EES and the associated "clipper chip" in the United States is another example of a technology chosen for explicitly political purposes.

Another aspect of the relationship between states and technology is that states have been involved in the development of many technologies. Technical innovation has usually been conducted by private firms, although governments, through public policy can act as facilitators for the development of new technologies. In the case of the United States the government, especially the Department of Defense, has been particularly active in assisting in the development of new technologies. One of many instances in which the United States government involved itself in technological innovation was Sematech. Sematech is a consortium composed of American semiconductor companies and

---

[66] Jos Huigen, "Information and Communication Technology in the Context of Policy Networks," Technology In Society 15.3 (1993): 327-338.

[67] Anthony Perl, "Public Enterprise as an Expression of Sovereignty: Reconsidering the Origin of Canadian National Railways," Canadian Journal of Political Science 27.1 (1994): 23-52.

was initially funded in part by the Department of Defense. The consortium was established in order to maintain and enhance American market dominance in the semiconductor industry.[68] In addition, the Internet, and other associated technologies were initially developed with the assistance of the United States Department of Defense, through its Defense Advanced Research Projects Agency (DARPA).[69]

In regard to the development of standards, there appears to have been a shift in structural power over standards development from state to private entities. Paul A. David and Mark Shurmer have documented a shift in standards development away from traditional public-private and national standards development organizations (i.e. the International Telecommunication Union (ITU)) to alliances or consortia composed of corporations such as the Object Management Group (OMG).[70] The formation of independent consortia is in response to the perceived slowness of other standards development organizations and the increased need of standards for information and communication technologies. In addition, some companies such as Microsoft and Intel, will release their products to gain significant market shares and then become *de facto*

---

[68] B.R. Inman, and Daniel F. Burton Jr., "Technology and Competitiveness: The New Policy Frontier," Foreign Affairs 69.2 (1990): 121. Note: Sematech's federal funding was withdrawn in the mid-1990's. Sematech Events: 1995, Sematech, 1 Feb. 1999 <http://www.sematech.org/public/general/timeline/95.htm>.

[69] Barry M. Leiner et al., Internet Society (ISOC) All About the Internet: A Brief History of the Internet, Internet Society (ISOC), 27 Feb. 1999 <http://www.isoc.org/internet/history/brief.html>.

[70] The Object Management Group (OMG) is a worldwide consortium of software companies. Paul A. David and Mark Shurmer, "Formal standards-setting for global telecommunications and information services: Towards an institutional regime transformation?," Telecommunications Policy 20.10 (1996): 803.

standards. Among the advantages of the consortia are that they can keep up with the pace of technical change. However, one significant disadvantage of consortia standards setting is that public concerns may not be taken into account when a standard is created. [71]

1.7: A Micro Level Perspective

As stated above states are in the process of undergoing significant change. A micro level perspective is also required in order to examine the orientations of the actors involved in the adoption of the DSS. A society-centered perspective can be used to complement a statist perspective. Cathie Jo Martin's investigation of corporate taxation policy in the United States uses a combination of state and societal perspectives. This method is termed "coalition model of state/society relations."[72] Some of the basic propositions of this perspective are that the state is not cohesive, but made up of factions. These factions are the result of the fragmented political institutions in the United States. These institutional factions also create alliances with societal interests and influence public policy.[73] The Advocacy Coalition Framework (ACF) developed by Paul A. Sabatier and Hank C. Jenkins-Smith may be especially useful in this regard, since it may be used to expand on Martin's theoretical framework.

---

[71] David and Shurmer 801-804.

[72] Cathie Jo Martin, "Business Influence and State Power: The Case of U.S. Corporate Tax Policy," Politics & Society 17.2 (1989): 190-191.

[73] Cathie Jo Martin 190-191, 198.

The ACF was developed in response to the prevalence of the "stages heuristic." The stages heuristic articulated that public policy formation proceeds along regular and defined steps. These steps include goal setting, agenda setting, compiling a list of all alternatives, examining all alternatives and then making a rational choice of the best policy and policy instruments that will best accomplish all goals. However, it was eventually realized that the stages heuristic could not adequately describe policy formation. The ACF has four basic tenets that form its foundation. The first is that observation and examination of policy change must be conducted over a period of at least ten years in order to examine the effects of policy-oriented learning. The ACF places a great deal of emphasis on policy-oriented learning as a means to influence and possibly change some elements of an advocacy coalition's belief system. Second, the focus of analysis should be on policy subsystems, which includes the participants who attempt to influence policy in a given policy area. Third, those participants from other levels of government should be included in any analysis of public policy formation. Fourth, the ACF emphasizes the belief systems behind advocacy coalitions and hence public policies.[74]

According to Sabatier, the ACF also considers stable and dynamic factors that impinge on a policy subsystem. There are four stable factors impinging on a policy subsystem. The stable factors are those that are consistent. The first stable factor is the nature of the problem, such as whether it involves a common

---

[74] Paul A. Sabatier, "Policy Change over a Decade or More," Policy Change and Learning: An Advocacy Coalition Approach, eds. Paul A. Sabatier, and Hank C. Jenkins-Smith (Boulder: Westview Press, 1993) 15-16.

resource, whether the area is conducive to policy-oriented learning, and public perceptions on the issue in question. The second stable factor is the distribution of natural resources. The third stable factor involves cultural values and social structure. The fourth stable factor is the legal structure. In the case of the United States, the legal structure would include those institutions established under the Constitution. The dynamic factors are factors that can change relatively quickly compared to the stable factors. The first dynamic factor is socioeconomic conditions and technology. The second dynamic factor is governing coalitions. The third dynamic factor is the impacts of other policy subsystems. The fourth dynamic factor includes public opinion.[75]

Under the ACF, the participants in the policy subsystem are divided into advocacy coalitions. The advocacy coalitions are held together by a belief structure comprised of core, near core, and secondary beliefs. The core beliefs are fundamental beliefs, which include ontological orientations. These beliefs are applied to all areas and are extremely difficult to change. The near core beliefs include beliefs on how to best achieve the core beliefs of an advocacy coalition. These beliefs are more narrowly focused than the core beliefs and they are difficult to change, but not impossible. The secondary beliefs encompass less important matters such as those dealing with preferred policy instruments and they are applied to specific policy areas. As opposed to the other belief levels, these beliefs can be easily changed.[76]

---

[75] Sabatier 20-23, 223-224.

[76] Sabatier 30-31.

Some elements and insights of the ACF can be adapted for a short-duration case study, as attempted in this paper. One criticism that Sabatier makes of statist theory is that states cannot act as cohesive and autonomous wholes, especially in the United States where many institutional and cultural factors preclude this possibility.[77] However, that does not preclude individual government agencies or small groups of individual agencies working in a cohesive and autonomous manner. In addition, the advocacy coalition concept is useful in arranging participants in a policy sub-system, since it can show underlying beliefs and motivations for opposing a particular course of action and why other courses of action may be preferred.

One problem in applying the ACF to this particular area is the relatively short period from the late 1980's to the early 1990's. However, the longer term outlook would not have effected the outcome in this case study. Another problem in applying the ACF would be the requirement for identifying distinct policy subsystems. The ACF does makes allowances for participants in other policy sub-systems to become involved in the policy sub-subsystem under consideration. However, as stated earlier, the justifications for distinctions between policy areas, such as broadcasting, telecommunications and computing are disappearing. Applying the ACF to this environment may be difficult since more actors from other policy sub-systems could become involved. These other participants may make it difficult to determine the belief systems of particular advocacy coalitions. Another

---

[77] Sabatier 37.

problem in applying the ACF to this policy area is the apparent lack of any policy-oriented learning. During the public comment period the NIST was shown comparative test results of the RSA algorithm and DSA. This evidence did not appear to have been persuasive. Under these circumstances, no policy-oriented learning could be expected to take place.

CHAPTER TWO: THE DIGITAL SIGNATURE STANDARD

2.1: Perceptions of State Control in Cryptography Policy in the United States

Many authors engaged in the scientific study of cryptology and journalists have alleged that elements of the United States government, namely the NSA, have been attempting to exercise influence over civilian cryptography since World War II. Some of the policies and actions employed by the government of the United States have had some degree of success in limiting the availability of strong cryptography.[78] The literature on cryptography policy cited below indicates that the American state and in particular, the NSA appears to have used three broad strategies to control civilian cryptographic technologies. These strategies and incidents are discussed in more detail below. First, the NSA and other national security interests attempted to widen their jurisdiction vis-à-vis other government departments where issues of information security were involved. Second, the NSA has been accused of attempting to exercise control over sources of civilian cryptographic knowledge and invention. The third measure has involved the use of export controls on certain products, both software and hardware, that use strong cryptography.

The best example of the first strategy employed by the United States national security apparatus was National Security Decision Directive (NSDD) 145 in 1984 and a later accompanying order from National Security Advisor, John Poindexter, expanding the scope of NSDD-145. These measures were intended to

---

[78] The term strong is intended to refer to cryptographic methods that are very difficult to attack. The term weak denotes cryptographic methods that are easily attacked.

increase the security of sensitive government information during the Cold War with the former Soviet Union. Under this directive, the responsibilities of the Department of Defense and other agencies, including the NSA, were expanded to include the protection of non-classified, but sensitive, government information.[79] Under this order, the director of the NSA was given expanded jurisdiction over areas such as standards, equipment, computer and telecommunications security. The new regulations covered other government departments and private corporations that possessed non-classified, but sensitive, government information.[80]

One of the means by which the NSA sought to restrict the use and complexity of civilian cryptography was to target civilian research conducted by academics. In the late 1970's, the NSA attempted to persuade the National Science Foundation (NSF) to surrender its authority over the allocation of funding for research projects that involved cryptography. The NSA argued that it had jurisdiction over the allocation of funding to cryptographic research projects. The NSF disagreed with the NSA and opposed its attempt to control the allocation of funds to cryptographic research. The NSF eventually allowed the NSA to review the technical merits of funding requests made to the NSF by those engaged in cryptographic research. Matters were further confused in this area when the NSA

---

[79] The NSA was instrumental in the passage of NSDD-145, as demonstrated by a de-classified U.S. government document. brooks.gif, Electronic Privacy Information Center (EPIC), 15 June 1998 <http://www.epic.org/crypto/csa/brooks.gif>.

[80] Diffie and Landau 66-67.; Bruce Schneier and David Banisar, eds., The Electronic Privacy Papers: Documents in the Battle for Privacy in the Age of Surveillance (Toronto: John Wiley and Sons Inc. 1997) 298-300.

also started to support cryptographic research itself. One researcher, Leonard Adleman, was offered funding by the NSA. Adleman was not keen to receive funds from the NSA, but the NSF refused to consider him for funding, since he had already received funding from the NSA. An accommodation was eventually reached where both the NSA and NSF would fund cryptographic research, and researchers were not obliged to accept NSA funding.[81]

Another method by which the NSA was perceived to have exercised control civilian cryptography in the late 1970's was through the Invention Secrecy Act. Under this legislation, patent applications on certain inventions could be sent to other government agencies, where the invention, if considered a possible threat to national security, could be deemed to be a secret. The legislation also had provisions for serious criminal sanctions if knowledge or the existence of the patent on the invention was circulated. The act was applied to a university professor, George Davida, and inventor, Carl Nicolai. Nicolai had invented a low cost mechanism designed to scramble telephone transmissions, while Davida had developed a cryptographic device. The NSA scheme backfired when Davida and Nicolai publicized their treatment and the classifications of their patents were subsequently removed. They successfully argued that the classifications had been

---

[81] Diffie and Landau 62-63.; Schneier and Banisar 294-295.; David Burnham, The Rise of the Computer State (New York: Random House Inc., 1983) 139-141.; James Bamford, The Puzzle Palace: A Report on America's Most Secret Agency (Toronto: Penguin Books, 1983) 441-444, 454-455.

mistakes on the part of the NSA, since their inventions had already received some publicity.[82]

Another area where the NSA was alleged to have been involved was in the development of the Data Encryption Standard (DES). The DES was developed in the late 1970's by the United States government as a standard to protect sensitive government and corporate information. The National Bureau of Standards (NBS), with assistance from the NSA, started to evaluate candidate algorithms that had been submitted. International Business Machines Corporation (IBM) submitted an algorithm called "Lucifer". IBM also made changes to the algorithm requested by the NSA. This algorithm eventually became the DES. The NSA involvement with the DES was a source of controversy since the NSA asked IBM to keep some of the design specifications secret and to shorten the key length of the algorithm that it submitted. Accusations were also made that the NSA had tampered with the DES in such a manner as to make the decryption of messages easier for the NSA. However, accusations that the NSA had improperly tampered with the DES were never substantiated.[83] The DES, despite lingering questions concerning its development, became a worldwide financial services standard. The NSA was also accused of quashing an attempt by the National Bureau of Standards (NBS) to develop a public key cryptographic standard in 1982.[84]

---

[82] Diffie & Landau 62.; Schneier and Banisar 295-296.; Burnham 138-139.; Bamford 446-451.

[83] Bamford 434-439.; Schneier and Banisar 293-294.; Diffie and Landau 59-60.

[84] United States, General Accounting Office (GAO), Communications Privacy: Federal Policy and Actions (Washington: General Accounting Office, 1993) 20.

In the early 1980's, NSA Director, Admiral Bobby Inman approached the American Council on Education in order to gain their assistance in limiting the dissemination of academic cryptographic knowledge concerning strong cryptography. Inman believed that there was an incompatibility between the free distribution of academic work concerning strong cryptography and national security.[85] The American Council on Education convened a study group comprised of representatives of the scientific community and a representative from the NSA. The study group rejected any idea on controls over the dissemination of academic information. However, the study group recommended a limited time project where authors could submit their papers, if they so desired, for review by the NSA. If the paper contained sensitive information, the NSA would request that it not be published. Despite the misgivings of many in the academic community the project was not as intrusive as many feared.[86]

Congress enacted the Computer Security Act of 1987 in order to create a division of powers regarding the protection of classified and non-classified information. This act was intended to keep the Department of Defense, and the NSA in particular, out of civilian standards setting and civilian information protection. The Department of Defense, and in particular the NSA, were given responsibility for the protection of classified government information. The NIST (formerly the NBS) was responsible for the protection of non-classified, but

---

[85] inman.article, Electronic Frontier Foundation (EFF), 8 Feb. 1982, 13 Aug. 1998 <http://www.eff.org/pub/Privacy/Old/inman.article>. Note: This article by Admiral Inman was originally published in February 8, 1982 edition of Aviation Week and Space Technology.

[86] Diffie & Landau 63.; Burnham 142.; Bamford 451-453.

sensitive, government information. The Computer Security Act did allow for collaboration between the agencies on technical matters. However as many observers have noticed, this agreement was undermined by an intra-governmental agreement between the NSA and the NIST in 1989. This intra-governmental agreement was the NSA/NIST Memorandum of Understanding (MoU). Under this agreement the NIST consulted with the NSA on all matters involving cryptography. In addition, a technical working group (TWG) was also established under the MoU with members from both the NSA and the NIST.[87]

Another mechanism that the United States government has used to retard the dissemination of cryptographic technologies is export controls. The NSA has been accused of being especially active in exercising export controls over advanced encryption technology. The NSA has some degree of power in determining whether or not an export permit is issued for cryptographic products.[88] The United States government maintains a number of lists, which identify items whose export is controlled. The United States Munitions List (USML) lists items that can be regulated due to their military applications. The laws which regulated the exportation of these items, including cryptographic software and hardware, were the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). The State Department administers these regulations. The AECA allows the President to restrict the export of munitions on the USML, while

---

[87] Diffie and Landau 70-71.; Schneier and Banisar 302-303.

[88] John Perry Barlow, "Decrypting the Puzzle Palace," Communications of the ACM 35.7 (1992) 25-31.

the ITAR is the enabling legislation setting out the items, either technology or commodities, which are to be regulated. Under United States law, any commodity that may have civilian or military uses is classified as a "dual use item." The Department of Commerce maintains a similar list of items called the Commerce Controlled List (CCL) which controls dual use items. The controls over items on the CCL are less severe than those items on the USML. Cryptographic hardware and software are classified as dual use items, and the export of any cryptographic hardware and software with a key size of over 40 bits requires a permit. There are exceptions to the 40-bit limit, since the United States law allows for the export of products with strong encryption to other countries under certain circumstances. In some cases, the export of products with DES is allowed to certain countries and financial institutions and if the exporting company makes commitments to develop technologies with key recovery.[89] The export of RSA for authentication and key exchange is allowed, however it is extremely difficult to legally export RSA-based products for encryption.[90] Export controls have proven to be a hindrance to the American software and electronic applications industries since businesses are forced to develop two product lines, one for domestic markets (including Canada[91])

---

[89] Electric Frontier Foundation (EFF), Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design (Sebastopol: O'Reilly & Associates, 1998) 1-4 - 1-5.

[90] "RSA Labs FAQ – Can RSA be exported from the United States?" RSA Laboratories, FAQ 4.0, RSA Data Security Inc., 3 March 1999 <http://www.rsa.com/rsalabs/faq/html/6-4-1.html>.

[91] Canada appears to be exempt from United States export controls on encryption items under the Export Administration Regulations (EAR) since no license is required to export encryption items that are to be used in Canada. Banking/financial Regulation, Bureau of Export Administration (BXA), 22 Sept. 1998, July 4, 1999 <http://www.bxa.doc.gov/Encryption/encbank.pdf>. Note: This publication was originally part of the Federal Register (vol. 63. No.183) notice of September 22, 1998.

and the other for export, which increases the costs for the industry. Many companies only develop products with weak encryption in order to satisfy the export control requirements. In 1996, responsibility over administering the export controls over civilian cryptographic technology was transferred to the Department of Commerce and its Bureau of Export Administration (BXA) from the State Department due to Executive Order 13026. Commercial software with encryption capabilities is now regulated under the Export Administration Act (EAA). The EAA is implemented by the Export Administration Regulations (EAR) which control items listed on the CCL. Recently, the President has used another piece of legislation called the International Emergency Economic Powers Act (IEEPA) to uphold the Department of Commerce's export controls, since the EAA is only temporary legislation. However, the Department of Commerce's restrictions on commercial cryptographic technologies are similar to the ones that existed under ITAR, since they consider security and foreign policy concerns when an export permit is issued.[92] One visible illustration of the effects of export controls can be found in web browsers, such as Netscape Navigator and Microsoft Internet Explorer (MSIE). Netscape and Microsoft are forced to manufacture two versions of their web browsers or provide software patches.[93] The domestic versions of Netscape and MSIE for the United States and Canada have a 128-bit encryption module. The export versions of Netscape and MSIE only have a 40-bit encryption

---

[92] 970825 decision, Electronic Frontier Foundation (EFF), 12 Jan. 1999 <http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/Legal/970825.decision>.

[93] A software patch is a computer program that updates or modifies another computer program.

module, in order to comply with US export controls. Opposition to export controls has come from numerous sources and various attempts have been made to minimize or remove export controls on encryption products.[94] Export controls have been challenged in the United States federal judicial system as being an unconstitutional prior restraint on free speech protected under the First Amendment of the Constitution.[95] Export controls have also been circumvented by other means. Corporations with international affiliates can circumvent export controls. This was demonstrated by a Network Associates Incorporated (NAI) venture to produce and distribute strong cryptographic software via a Dutch company.[96] In addition, the Internet also allows persons and businesses to circumvent the United States government's export restrictions. Even the Netscape and MSIE browsers with 128-bit encryption modules or software patches that upgrade the cryptographic modules are available for downloading from foreign WWW and FTP sites.[97]

---

[94] For instance see: gephardt-letter-498.html, Internet Privacy Coalition, 2 April 1998, 13 Aug. 1998 <http://www.crypto.org/gephardt-letter-498.html>.

[95] One such case is Bernstein v. U.S. Department of State et al. In the Bernstein case, the federal district court ruled that export controls under both ITAR (Bernstein II) and under the Department of Commerce (Bernstein III) were an unconstitutional prior restraint on first amendment rights. However, the declaratory relief was only limited to Bernstein and the encryption program that he wrote called Snuffle. 970825 decision, Electronic Frontier Foundation, 12 Jan. 1999 <http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/Legal/970825.decision>. An appeal court has upheld the lower court's decision in this case. Declan McCullagh, "Landmark Ruling on Encryption," Wired News 6 May, 1999 <http://www.wired.com/news/news/politics/story/19553.html>.

[96] Network Associates Announces Availability of 128bit PGP Encryption Software for Global Customers, Network Associates Incorporated (NAI), 20 Mar.1998, 13 Aug. 1998 <http://www.nai.com/about/news/press/1998/march/032098.asp>.

[97] See: Replay Associates, Replay Associates L.L.P., 21 March 1999 <http://www.replay.com>.

Another situation in which the NSA was perceived to have attempted to prevent the dissemination of cryptographic knowledge by the academic community was to stop the presentation of academic information and papers at conferences. The most noteworthy and often cited use of this approach occurred in 1977. A NSA employee on his own initiative had contacted the Institute of Electrical and Electronics Engineers (IEEE) in regard to the material that was to be presented at an upcoming conference. This material included information concerning public-key cryptography. The IEEE was told that the presentation of the material could be construed as a violation of export control laws. The employee had not informed the IEEE of his affiliation with the NSA. However, when this fact was discovered, the IEEE planned to have the materials and information presented anyway. The NSA then indicated that the warning was a mistake, and that the employee's warning did not reflect official NSA views. The NSA itself was subsequently cleared of any wrongdoing.[98]

Former NSA Director, Admiral Bobby Inman, denied that the NSA attempted to subvert civilian cryptographic research and innovation in the above incidents. He stated that it was difficult for national security interests to act in order to take precautions that they felt were justified. He believed that federal wiretapping laws and other legal protections limited the ability of national security and law enforcement agencies to conduct domestic surveillance. Inman further believed that there should have been more consideration for the views of national security

---

[98] Diffie and Landau 61-62.; Bamford 444-446.; Schneier and Banisar 295.

interests in cryptography policy and even encouraged the participation of the academic community in the process.[99] Inman's comments strongly suggest that he thought that there was a lack of state autonomy and power to act in this particular area. Inman appears to have believed that security and law enforcement agencies were precluded from taking appropriate actions to increase security over sensitive government and scientific information.

2.2: The Development of the Digital Signature Standard

A great deal of the research that has been conducted on cryptography policy in the United States, including the DSS, appears to have focused on the involvement of the NSA. The involvement of the NSA is perceived in a negative context since many persons believe that the NSA's involvement was in contravention of the Computer Security Act of 1987 since the objective of the act was to keep state security agencies out civilian standards setting.[100] One examination based on documents obtained under the Freedom of Information Act (FOIA) by the Computer Professionals for Social Responsibility (CPSR) noticed that the NSA was heavily involved in the development of the DSS, and even chose the El Gamal[101] algorithm which was used as a basis for the DSS. Many believe

---

[99] B.R. Inman, "The NSA perspective on Telecommunications Protection in the Nongovernmental Sector," The Electronic Privacy Papers: Documents in the Battle for Privacy in the Age of Surveillance, eds. Bruce Schneier and David Banisar (Toronto: John Wiley and Sons Inc. 1997) 347-355.

[100] For instance: David L. Sobel, "Government Restrictions on the Development and Dissemination of Cryptographic Technologies: The Controversy over the Digital Signature Standard," Computer Law Reporter 16.256 (1992): 265-270.

[101] El Gamal refers to a mathematical algorithm that can be used for generating and verifying digital signatures.

that El Gamal was chosen over the main commercial algorithm RSA, since the NSA feared that RSA could be used for strong encryption, while El Gamal could only generate and verify digital signatures.[102] The documents also show that there was a considerable amount of contention between the NIST and the NSA in the development of public key cryptographic standards.[103]

The NIST had proposed a number of digital signature and hashing algorithms to the NSA for their review. There appears to have been some tension regarding the NSA's response to the algorithms submitted. As mentioned before, the NSA ultimately submitted another public key algorithm based on the El Gamal algorithm, which they forced the NIST to adopt as the proposed DSS.[104]

The NIST conducted a preliminary examination of some digital signature algorithms. Four algorithms that were initially examined by the NIST were the Schnorr algorithm[105], Shamir algorithm, the RSA algorithm and a variant of the RSA algorithm.[106] The algorithms were to be evaluated on their technical aspects, viability to industry and costs associated with their implementation.[107] In reviewing

---

[102] This is noticed by some accounts. See: David Stipp, "11.11.96 TECHNO HERO OR PUBLIC ENEMY?" Fortune, 11 Nov. 1996, 7 Oct. 1998 <http://pathfinder.com/@@qPRqOwYA60VQwxah/fortune/1996/961111/rsa.htm>. Note: The DSA actually can be used for encryption. The method is described by Bruce Schneier. Schneier 490.

[103] David L. Sobel, New NIST/NSA Revelations, Electronic Privacy Information Center (EPIC), 22 July 1998 <http://www.epic.org/crypto/dss/new_nist_nsa_revelations.html>.

[104] Those who have researched cryptography policy in the United States have noticed this fact. Diffie and Landau 72.; Schneier and Banisar 305-306.

[105] The Schnorr algorithm was a variant of the El Gamal algorithm.

[106] This was the RSA algorithm with the Chinese Remainder Theorem.

[107] F. Lynn McNulty, and Dennis K. Branstad, memorandum for Raymond G. Kammer, 21

the candidate algorithms, "the most important consideration [was] providing the maximum amount of security with minimal cost and minimum requirements for trusted third parties."[108] According to one source, the RSA algorithm and the RSA variant had many advantages. One advantage was that they generated all of the parameters that were used in digital signatures so that a third party would not have to be involved in this part. The RSA variant was also seen as the cheapest to use. All of the algorithms were evenly matched in terms of implementation in software and storage requirements.[109]

The sentiment that RSA was the best algorithm was not shared by all. One person who appeared to think otherwise was Dr. Jim Omura, president of Cylink, a subsidiary of Caro-Kahn Incorporated one of the companies involved in Public Key Partners (PKP). RSA Data Security Incorporated and Cylink collaborated to form PKP. This alliance claimed they held the patents, both domestic and foreign, on all public key cryptographic technologies and methods, including the RSA algorithm. PKP also claimed that it held patents that covered the El Gamal algorithm.[110] The

---

Nov. 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC. Note: This memo had a recommendation for an algorithm to be used in the FIPS. However, the recommendation appears to have been edited out.

[108] F. Lynn McNulty, and Dennis K. Branstad, memorandum for Raymond G. Kammer, 21 Nov. 1990.

[109] F. Lynn McNulty, and Dennis K. Branstad, memorandum for Raymond G. Kammer, 21 Nov. 1990.

[110] Robert B. Fougner, letter to Dennis K. Branstad, 20 April 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.; Schneier 604-605.

alliance between the two companies was ultimately terminated.[111] PKP had been lobbying especially hard for RSA to be adopted as the proposed DSS. Dr. Omura's thoughts on the matter were revealed in one memo which stated:

> he [Dr. Omura] still felt that it [El Gamal] is technically superior, but that the public acceptance of RSA within the U.S. and Europe compelled him to strongly recommend RSA as a signature standard.[112]

The United States government had prior dealings with RSA and RSA Data Security. The United States Government, through the Department of Defense, had funded the research that ultimately led to the development of the RSA public key cryptosystem. Under this arrangement the United States government was permitted to use the RSA algorithm on a royalty free basis. In the early 1990's, the Office of the Secretary of Defense (OSD) was in the process of negotiating with RSA Data Security for a license to use and modify their products for use in the OSD. During this time, there was an awareness by RSA of the work of the NIST and the NSA on public key cryptographic standards. It appears that the agreement between RSA Data Security and the OSD started on February 14, 1990 and subsequently extended on February 26, 1990. RSA Data Security did not deliver the goods that it was required to by a certain date. Due to an administrative problem, RSA Data Security was never paid for the license under the extended agreement and the deal appeared to have fallen through. However, it appears that the United States government still possessed RSA source code from the first

---

[111] David Stipp, "11.11.96 TECHNO HERO OR PUBLIC ENEMY?" Fortune, 11 Nov. 1996, 7 Oct. 1998 <http://pathfinder.com/@@qPRqOwYA60Vqwxah/fortune/1996/961111/rsa.htm>.

[112] Dennis K. Branstad, memorandum for the record, 27 Apr. 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

agreement. In May 1991 another Department of Defense agency, the Defense Logistics Agency (DLA) was given responsibility for developing technologies for electronic transactions. DLA then designated another organization, the Logistics Management Institute (LMI) the responsibility of re-acquiring a license from RSA Data Security. However, there was some question about whether RSA Data Security would be willing to grant another license and whether the LMI could actually procure the license. In the initial negotiations over acquiring a license for RSA between RSA Data Security and the OSD the language used in the contract required six months of negotiation.[113] One memo from the NIST clearly indicates that they believed that they should not have to purchase another license for another technology, the El Gamal algorithm, patented by PKP, in order to use it in a standard for digital signatures.[114] The confusion surrounding the United States Department of Defense's dealings with PKP and the problems negotiating for the license and problems with obtaining another license for an algorithm controlled by PKP, may have made the United States government wary of future dealings with PKP and RSA Data Security.

In order to use the RSA algorithm as the DSS, those who wished to use it would have had to obtain a license from PKP. There was willingness on the part of PKP to grant licenses for the use of the RSA algorithm "on reasonable terms and

---

[113] Memorandum for the record, 13 March 1991, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

[114] Dennis K. Branstad, memorandum for the record, 27 Apr. 1990.

conditions on a non-discriminatory basis,"[115] if it was selected as the DSS. It was also unclear to the United States government whether PKP would grant licenses for the use of the El Gamal algorithm and the Diffie-Hellman key exchange mechanism, on which PKP also claimed the ownership of the patents.[116]

In the course of developing the proposed DSS, the NIST received a letter from one Roger Schlafly who was against the NIST adopting a public key standard controlled by PKP. Included within the letter were several bases for the author's position. First, Mr. Schlafly questioned whether a mathematical algorithm could be patented. Second, he thought that PKP was attempting to monopolize public key cryptographic technology. If the government adopted a PKP standard it would have led to a state-sanctioned monopoly. Third, there was a question of whether PKP would grant licenses under fair conditions. Schlafly stated that in the past PKP had refused to issue licenses to potential competitors. Fourth, he also claimed that PKP did not charge fair royalty fees. According to the Schlafly, the minimum initial royalty charge was $25,000 and the minimum payment per year was $10,000. He perceived these high fees as an obstacle to the development of software by small companies. In addition, he argued that PKP engaged in unfair competitive practices. However, one option that he suggested was that in return

---

[115] James Burrows, memorandum for Raymond Kammer, 30 May 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

[116] James Burrows, memorandum for Raymond Kammer, 30 May 1990.

for the use of PKP products as federal government standards, PKP would renounce any claims to royalties.[117]

If the NIST had adopted the RSA algorithm as the DSA instead of the EL Gamal algorithm, it would have conformed to Scott Turner's expectations. As mentioned before, Scott Turner believed that state/corporate relationships could be both cooperative and adversarial and that cooperative relationships between states and corporations could reduce state autonomy. The proposed DSS could have been an example of state-corporation cooperation that enhanced corporate power while reducing state autonomy. If RSA had been adopted as the United States government standard for digital signatures, it would have added to its position and reputation as a *de facto* world standard. In addition, RSA Data Security Inc. would have had the ability to collect more licensing fees and royalty payments for the use of its algorithm. Instead, the United States government acted contrary to Turner's expectations by developing an alternative royalty-free standard for digital signatures that could be available for anyone to use.

The selection of the El Gamal algorithm is also consistent with Huigen's observations that the selection and implementation of technologies is an inherently political process. If technical considerations alone had been considered in the adoption of the DSS, it is most likely that the RSA algorithm would have been adopted. However, since the government agencies involved wanted a royalty-free DSS, they based the DSS on another algorithm. The preferred choice of United

---

[117] Roger Schlafly, letter to NIST, 11 Oct. 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

States government agencies had implications for the design of digital signature applications. The El Gamal algorithm could generate a digital signature fairly efficiently, however, verification would take longer than with other algorithms. The NIST believed that the proposed DSS would be especially useful in "smart cards". The digital signature could be performed by the smart card, since the card would contain all of the elements needed to perform the digital signature, while verification would take place in machines that had greater computational power since more computer resources could be devoted to verification. Apparently, this proposed platform for DSS use was considered relatively early.[118] Many persons and organizations offering comments concerning the proposed DSS thought that this implementation would not work as intended.

Application of the ACF to the NSA/NIST is problematic. It is difficult to determine the core values of this advocacy coalition or even whether the NSA/NIST constituted an actual advocacy coalition. The core value of the NSA could have included security. The NSA could have seen the widespread distribution of RSA as a possible security threat since it could be used for encryption as well as digital signature generation and verification. It is also difficult to determine the ontological orientations of these agencies precisely. An argument could be made that the NSA had a negative perception of human nature, based on their perceived efforts to exercise influence over and limit cryptographic

---

[118] Dennis Branstad, memorandum for John Lyons, 6 July 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.; A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), Electronic Privacy Information Center (EPIC), 30 Aug. 1991, 9 July 1998 <http://www.epic.org/crypto/dss/dss_fr_notice_1991.html>.

development. However, no clues are given concerning the NIST's basic ontological positions. In regard to near core beliefs, one plausible belief of this advocacy coalition is that of the government having a legitimate role in standards setting. The secondary aspects could include the legitimate use of the FIPS process in influencing the adoption of an alternative standard for digital signatures.

The public responses both from other departments and agencies of the United States government and from industry exhibit a variety of divergent opinions regarding the DSS. The public comments are more diverse than other accounts of cryptography policy have suggested.

2.3: Government Responses to the DSS

In regard to the government responses, there was a wide degree of variation. Some agencies wholeheartedly supported the proposed DSS, while others supported the DSS, but expressed some concerns. Some comments from other agencies appeared to criticize the proposed DSS. Other agencies sent submissions indicating that they had no comments in regard to the proposed DSS and some agencies indicated that they would adopt it without question.[119]

---

[119] Some of these agencies included the United States Government Printing Office, the Railroad Retirement Board, the United States Small Business Administration and the Panama Canal Commission. Vincent F. Arendes, letter to James H. Burrows, 18 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Dale G. Zimmerman, letter to James H. Burrows, 8 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Lawrence E. Barrett, letter to James H. Burrows, 14 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Joseph J. Wood, letter to James H. Burrows, 20 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

The Department of Commerce[120], the Defense Information Systems Agency[121], the Department of Justice[122], and the General Services Administration[123] supported the adoption of the proposed DSS. In addition, the Department of the Navy indicated that there would be a slight cost to the United States Marine Corps (USMC) if the proposed DSS were adopted. However, they did not oppose the adoption of the DSS.[124]

Other government agencies were supportive of the proposed DSS, but had concerns. The comments received from the Department of Education indicated that they did not presently use any digital signature technologies. However, they suggested that they might adopt a public key system in the future. The Department of Education indicated that elements of the proposed DSS and other

---

[120] Reed Phillips, memorandum for James H. Burrows, 27 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[121] C.J. Pasquariello, letter to James H. Burrows, 28 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[122] Roger M. Cooper, letter to James Burrows, 28 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[123] Fred L. Sims, letter to James H. Burrows, date obscured, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[124] H.W. Jenkins, memorandum for Director NCSL, 18 Dec. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

related materials could assist them in developing and instituting a digital signature system.[125]

The Department of the Treasury also supported the proposed DSS, but noted some technical problems, such as the lack of a hashing algorithm. In their submission, the department indicated that they required assistance in finding a role for the proposed DSS, and implementing it in the projects in which they were involved. They indicated a willingness to work with the NIST regarding the application of the proposed DSS. However, the Department of the Treasury indicated that if they did not get satisfactory support, they would turn to the private sector for solutions.[126] The Internal Revenue Service (IRS) was also supportive of the proposed DSS, but had concerns about the availability of products that used the proposed DSS that had been screened by the NIST.[127]

The National Aeronautics and Space Administration (NASA) was also supportive of the proposed DSS. NASA noticed that the benefits of the DSS could include guaranteeing data integrity and authentication. However, their submission noted many areas of concern. These problems included the availability of skilled personnel for implementation of the DSS. NASA also noted that there was need

---

[125] Trish Liggett, letter to James H. Burrows, 22 Nov 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[126] Steven W. Broadbent, letter to James H. Burrows, 4 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[127] David L. Gaugler, memorandum for James H. Burrows, 30 Oct. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

for a hashing algorithm and that the administration of a key distribution system would entail more costs. Other areas of concern were the definition of a trusted third party, whether departments would be responsible for developing and implementing their own hardware and software with the DSS, technical concerns about the algorithm, and the advantages of using the DSS over other mechanisms such as passwords. In addition, NASA also wondered if an encryption function was also required.[128]

The United States Nuclear Regulatory Commission (NRC) was also supportive of the idea of a DSS, but noted that it had no present need for the proposed DSS. They indicated that some elements of their organization used the DES for communications security. However, the agency had some concerns with the proposed DSS. The NRC thought that the purposes of the DSS, including authentication should be clearly distinguished from data encryption or other forms of electronic identification. The commission's submission also indicated that there was concern over the costs of administration and implementation of the system. In regard to implementation, the NRC identified issues such as interoperability and compatibility with other systems, and the ease and transparency of use.[129]

The Federal Maritime Commission's submission noticed that the proposed DSS was too technical. According to the commission a standard and

---

[128] Lynwood P. Randolph, letter to James H. Burrows, 18 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[129] Gerald F. Cranford, letter to James H. Burrows, 27 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

accompanying information that was more understandable and user-friendly was required. They also recommended that encryption be reviewed in the literature accompanying the DSS.[130]

The Department of Energy was supportive of the idea of a DSS, but submitted a letter from one of their personnel that contained a number of concerns about the proposed DSS.[131] The criticisms of the proposed DSS included that it could only be used to generate and verify digital signatures. The submission strongly suggests that a DSS should be capable of other functions, such as encryption. The lack of a hashing algorithm was another problem since the author believed that it could result in an expenditure of government funds to remedy any problems associated with incorporating the hashing function into the DSS at a later date. Another problem was that the proposed DSS was not adequately secure. The comments also suggested that there be more comparative study of both the DSS algorithm (El Gamal) and the RSA algorithm. In addition, the comments did not criticize the involvement of the NSA, but suggested that civilian cryptographic experts should examine the algorithm proposed for the DSS. The submission

---

[130] Doris J. Spencer, letter to James H. Burrows, 29 Jan. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[131] Raymond S. Barrow, letter to James H. Burrows, 21 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

indicated that this process would take some time if the algorithm for the proposed DSS were to gain acceptance.[132]

The United States Agency for International Development did not challenge the proposed DSS directly, but noticed that there could be negative repercussions for the agency if it was adopted and its use made mandatory. The Agency was already in the process of implementing RSA based products and had committed a substantial amount of money ($100,000) to this project. The proposed DSS also posed a problem since it was incompatible with the RSA algorithm. The agency also appears to have been concerned about the extra costs involved in supporting both the proposed DSS and the RSA algorithm.[133]

Another government agency that was critical of the proposed DSS was the Department of Housing and Urban Development (HUD). HUD was concerned about the uncertain patent situation surrounding the algorithm for the DSS and the implications that this issue could have on implementation and use in products. HUD was also concerned about the computer resources required for using the proposed DSS. Support for the DSS and key management and distribution were other sources of concern for HUD. HUD was also in the process of implementing an electronic data interchange (EDI) system that could include encryption. HUD

---

[132] Gerald R. Johnson, letter to John P. Murphy, 27 Oct. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[133] John F. Owens, memorandum to James H. Burrows, 1 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

believed that the implementation of DSS in this situation could be complicated since it could not be used to encrypt data.[134]

A response to the proposed DSS submitted by a representative of the Food and Drug Administration (FDA) was particularly interesting. The comments were from the FDA's Director of the Office of Information Resources Management. The comments stated that the FDA was opposed to the proposed DSS on the grounds that it was too costly to implement and administer. In addition, the FDA was also opposed to the DSS since the director believed that passwords to private keys could be lost or compromised. The director seemed to indicate that in his opinion, hand written signatures were superior in detecting forgery.[135] This response begs the question of whether the FDA's information technology personnel had a full understanding of digital signature technology.

Applying the ACF to those government entities that supported and opposed the proposed DSS is difficult due to the diversity of comments regarding the proposed DSS. No real indications are given about the core, near core or secondary aspects of any belief systems. None of the agencies or departments could be said to form a cohesive advocacy coalition. They may have had similar comments about the proposed DSS, such as technical problems, costs of implementation and administration, ease of use, and others, but this does not

---

[134] Donald C. Demitros, letter to James H. Burrows, 6 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[135] Thomas E. Reddin, memorandum to Director, Office of Organization and Management Systems- Public Health Service, 20 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

indicate the presence of any coherent belief system. The problem of determining values is compounded since some government organizations did not elaborate on the reasons why they supported the adoption of the proposed DSS.

2.4: Industry Responses

Like the government responses to the DSS, the industry response also showed a great deal of variation. The majority of businesses and other organizations were aware of the technical shortcomings of the DSS. However, there were also some differences regarding what should be done with the proposed standard. In addition, a few businesses and a standards organization actually supported the adoption of the proposed DSS.

M. Blake Greenlee Associates Limited was one business that supported the adoption of the proposed DSS. According to their submission, the DSS could be used for non-repudiation and many other beneficial applications. This submission appeared to support the implementation of DSS in smart cards as suggested by the NIST. According to the submission, the use of the RSA algorithm in smart cards was more expensive. The submission also noticed that the American National Standards Institute (ANSI) was considering algorithm used in the DSS as a potential standard and that the DSA had also been submitted to the International Standards Organization (ISO) as a potential standard for international banking. In regards to NSA involvement, M. Blake Greenlee Associates did not see that as a negative implication. In fact, they thought that NSA involvement was beneficial since the NSA could deploy more expertise and resources in assessing the

proposed DSS. In addition, it was their belief that the government would have no interest in trying to undermine the DSS by intentionally weakening it. This referred to the alleged presence of a weakness in the proposed DSS, which would make the algorithm less secure and the digital signature more susceptible to forgery.[136]

Lemcon Systems Incorporated was another company that supported the adoption of the proposed DSS. However, Lemcon also noted that there were some problems with the proposed DSS. One problem was that of decertification, if the private key of a person was compromised. This involved a concern that documents that were "digitally signed" prior to the compromise of a particular private key would no longer be valid. Their submission seemed to imply that a time stamping mechanism should be included to protect documents signed prior to the compromise of a private key. Another concern of Lemcon was key certification. This concern involved a third party that would guarantee that a digital signature was made with a particular private key. The liability concerning documents signed with a digital signature was yet another source of concern to Lemcon.[137]

Information Resource Engineering Incorporated also made a submission in support of the proposed DSS. Their reasons for supporting the proposed DSS

---

[136] M. Blake Greenlee, letter to F. Lynn McNulty, 10 Jan. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[137] Thomas C. Jones, letter to Miles Smid, 24 Feb. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

were that it could produce lower cost products and that it could be used "in a wide variety of computing devices."[138]

Prime Factors was another company that also offered conditional support of the proposed DSS. The sentiment expressed in this submission was that the United States government, through the NIST, had a valid and vital role in establishing commercial cryptographic standards and that the new standard should be "public domain." Relying on past experience with the DES, the submission noted that without the United States government's attempts to provide cryptographic standards, secure communication methods might not have been developed. However, its support of the proposed DSS was contingent on the soundness of the algorithm.[139]

VISA was another company that offered support of the proposed DSS, but no endorsement. VISA was interested in a public key standard for the financial services industry and the proposed DSS was another standard from which to choose. VISA supported the royalty free use of the DSS and that it be covered by the less restrictive Department of Commerce export controls.[140]

---

[138] Anthony A. Caputo, letter to Director, Computer Systems Laboratory, 24 Sept. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[139] Michael Schwartz, letter to Director, Computer Systems Laboratory, 12 Sept. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[140] Bill Chen, letter to Director, Computer Systems Laboratory, 3 Mar. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Another organization expressing an interest in the proposed DSS was the X9 Accredited Standards Committee. The X9 committee is a sub-committee of the American National Standards Institute (ANSI). The X9 committee specifically deals with standards used in the financial services industry. The NIST/NSA were actively trying to cultivate allies in the standards community to adopt a DSS that was similar to the one that they were proposing. With the acceptance of the standard from a body such as X9, they could encourage the use of the proposed DSS in the United States and abroad. A meeting between NIST and NSA officials and X9 committee members was held in which the committee members were shown the proposed DSS. The X9 committee was supportive and encouraged the proposed DSS to be adopted. The X9 committee was in the process of developing a standard similar to the DSS. They stated that they would change the draft standard to conform to the approved DSS. Then it would be submitted to the membership for adoption.[141] ANSI eventually adopted digital signature standards based on both the DSS (ANSI X9.30) and RSA algorithms (ANSI X9.31).[142]

The evidence above concurs with the analysis discussed by Martin. State actors had support from some elements of the private sector. These organizations included VISA and the X9 committee of the ANSI. The degree to which these participants constituted an advocacy coalition is problematic. Like the government

---

[141] Harold G. Deal, letter to F. Lynn McNulty, 17 Jan. 1992, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[142] "RSA Labs FAQ – What are ANSI X9 Standards?" RSA Laboratories, FAQ 4.0, RSA Data Security Inc., 21 Feb. 1999 <http://www.rsa.com/rsalabs/faq/html/5-3-1.html>.

organizations, application of the ACF to the companies that supported the proposed DSS is difficult. It is difficult to determine the core values of some of the participants from many of the submissions. However, it is possible to determine some of the core values found in the submissions. The core value embodied in the Prime Factors submission was order. The submission states that the NIST's standardization efforts made the use of encrypted communications possible in the financial sector. This is apparent in the following quote from the Prime Factors submission:

> Without NIST standardization there would be a chaos of software and hardware "proprietary" algorithms ... Without the DES there would be no international Credit and Debit card ATM sharing networks (e.g. VisaNet, Plus, MasterCard, ATM, Cirrus). There would be no standardized method for financial institutions to securely transfer funds to the Federal Reserve.[143]

In regard to near core values, these organizations considered government involvement in standards setting legitimate. This was made explicit in the submission from Prime Factors. In regard to secondary aspects, these organizations felt that the FIPS process was a legitimate process for designing a standard for government, business and public use.

One of the most involved submissions against the adoption of the proposed DSS was from Addison M. Fischer, president of Fischer International Systems Corporation. Mr. Fischer had numerous objections to the proposed DSS. The objections included that the DSS was not widely used compared to RSA and that RSA would continue to be the world standard despite the U.S. government's

---

[143] Michael Schwartz, letter to Director, Computer Systems Laboratory, 12 Sept. 1991.

attempts to institute a different standard. Standards bodies such as the International Standards Organization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT)[144] of the International Telecommunication Union (ITU) had recognized the RSA algorithm as a standard. In addition RSA was also recognized as an international banking standard, and was also endorsed by French and Australian standards bodies. RSA was also widely used on the Internet. Another advantage to RSA was that it had significant market support since many companies that developed electronic networks and the applications used in electronic networks used RSA. In addition, RSA could also be used for encryption and thus data security, unlike the proposed DSS. Another problem with the proposed DSS was that it had many technical problems. One technical problem was that verification took longer than RSA. The submission from Fischer International Systems also noted that there were disadvantages for American business, government, and consumers if the proposed DSS was adopted. These disadvantages included the extra costs in terms of money and computer resources associated in supporting both the RSA algorithm and the proposed DSS. Both standards would need to be supported by American industry in order to conduct business with the American government and internationally. The submission also expressed concerns about how well American software would sell if it had to incorporate both standards. Incorporating both standards would have made the software more difficult to use and would have required more

---

[144] The CCITT is now known as the ITU's Telecommunication Standardization Sector (ITU-T)

computer resources. Other topics that Mr. Addison addressed were that civilian cryptographic experts had questioned the soundness of the proposed DSS and that its patent situation was uncertain.[145]

International Business Machines Corporation (IBM) was also opposed to the adoption of the proposed DSS. IBM had many technical problems with the proposed DSS. However, IBM also argued that the ISO/IEC 9796 standard, based on RSA, should be adopted as the government standard for generating and validating digital signatures or be a valid substitute.[146] The submission from Xerox also concurred with the IBM submission in calling for the adoption of the existing ISO 9796 standard instead of a different standard.[147]

Microsoft Corporation explicitly stated that in the absence of government action in this area, industry had adopted its own standards and that adoption of the proposed DSS by industry was not feasible as demonstrated by the following statement from Microsoft's submission:

> ... Given the lack of a DSS from the government for some time, the computer industry has, *de facto*, [sic] created its own digital signature standards. ... The government's late publication of its proposed DSS, together with its use of an unknown and untested algorithm makes it difficult, if not impossible, for

---

[145] Addison M. Fischer, letter to James H. Burrows, 26 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[146] Robert H. Follett, letter to James H. Burrows, 25 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[147] Russell D. Housley, letter to James H. Burrows, 26 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

> private and commercial organizations to adopt the government standard. ...[148]

Microsoft thought that the best course of action for the United States government was to abandon its current proposed DSS and adopt a new standard, preferably one that enjoyed industry acceptance. However, Microsoft also indicated that the period for public comment should be extended.[149]

Digital Equipment Corporation had many of the same technical concerns as the other respondents. Digital also indicated that it supported the RSA based system since it met their anticipated customer expectations. However, Digital did not completely rule out use of the algorithm used in the DSS as demonstrated by the following statement from their submission:

> Based on our review of the proposed DSA [Digital Signature Algorithm], we recommend that the applicability of the standard be narrowed to smart card-based funds transfer applications where a limited number of verifications will be required per signature, and where the verifications do not have to be preformed by centralized systems shared by large numbers of users.[150]

Digital Equipment Corporation also called for the establishment of a broader public key standard that could be used for other purposes.[151]

The submission from General Electric Information Services (GEIS) was also critical of the proposed standard on technical grounds. However, GEIS

---

[148] Nathan P. Myhrvold, letter to James H. Burrows, 21 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[149] Nathan P. Myhrvold, letter to James H. Burrows, 21 Nov. 1991.

[150] Morrie Gasser, letter to James H. Burrows, 18 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[151] Morrie Gasser, letter to James H. Burrows, 18 Nov. 1991.

recommended that the proposed DSS be revised so that it could use the RSA algorithm as well as the algorithm used in the proposed DSS. In addition, GEIS also suggested that the proposed DSS should be expandable in order to integrate new algorithms that may be developed in the future.[152]

Other comments, such as those from the CPSR were more concerned with the process by which the proposed DSS had been developed. There was particular concern about the involvement of the NSA in developing the standard. CPSR had submitted a Freedom of Information Act (FOIA) request to the NIST, which sought documentation concerning the development of the DSS. NIST officials refused this request. CPSR had also initiated legal action against the United States government in order to have National Security Directive 42 released for public inspection. This directive contained the United States government's policy agenda for computer security under the Computer Security Act and the involvement of the NSA in that regard. CPSR argued that the period for public comment should be extended so that information concerning the development of the proposed DSS could be released and examined by the public, before commenting on the proposed DSS.[153] Other comments by businesses, such as Digital Communications Associates Incorporated also echoed this concern.[154]

---

[152] Lew Priven, letter to James Burrows, 25 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

[153] Marc Rotenberg and David Sobel, letter to Director, Computer Systems Laboratory, NIST, 24 Oct. 1991.

[154] Marc Rhodes, letter to James H. Burrows, 27 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Some of the individual comments regarding the proposed DSS also had the same concerns.[155]

Again, there are problems in applying the ACF to the organizations and individuals who submitted comments against the proposed DSS. The core values of many of the corporations involved would include corporate freedom. In regard to near core beliefs, these corporations may have thought that this form of government involvement on this particular area may have been legitimate, but disagreed with the standard itself. Many of the submissions of the companies imply that the corporations thought they should be responsible for determining what standards are used. However, it is difficult to determine their thoughts about the role of government in electronic networks. They thought that the United States government should adopt RSA as a FIPS and some companies, such as Digital and GEIS, did not completely dismiss the applicability of the proposed DSS. However, they appear to have believed that the government should follow the lead of industry when deciding on standards in this particular area. This indicates that they believed that the preferences of industry were paramount. The secondary

---

[155] George H. Allen, letter to James H. Burrows, 20 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Andrew P. Black, letter to James H. Burrows, 21 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Richard Fall, letter to James H. Burrows, 19 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Lorraine Petrie, letter to James H. Burrows, 20 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Michael Sattler, letter to James H. Burrows, 11 Dec. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.; Miles D. Waldron, letter to James H. Burrows, 20 Nov. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

aspects of the corporations' belief structure may have included the belief that the use of the FIPS process to indirectly enact government preferences was wrong.

Applying the ACF to the groups and individuals concerned about the NSA's involvement is difficult since it is hard to determine whether they constituted an actual advocacy coalition. The core belief motivating CPSR and others concerned about the involvement of the NSA may have included accountability since they were concerned about the improper involvement of the agency in developing the standard. The NSA's involvement was suspect since it was involved far beyond its mandate under the Computer Security Act of 1987. A few of the individual responses also made reference to the Computer Security Act of 1987. The near core beliefs of these actors may have included a belief that they were entitled to full information about the development of the standard and the role of the NSA before submitting comments about the proposed DSS. In regard to secondary aspects, the CPSR and others believed in the use of the FOIA and the use of litigation to achieve their ends of having the pertinent information released.

Despite the misgivings of many in the private sector, the DSS was adopted as a United States government standard (FIPS 186) in 1994. The NIST had prepared responses to the criticisms directed against the proposed DSS. In regard to the time period and the openness to the public, the NIST stated that all laws and procedures had been followed and that the NSA had been involved only in a technical role. As for the comment period, NIST had allowed three more months than the original three month public comment period. The NIST also stated that no encryption capacity was required since the DSS was to be used for digital

signature generation and verification. As for a hashing algorithm, the NIST stated that one had been provided as a separate standard. This standard was the Secure Hash Standard (SHS) (FIPS 180). In regard to the security, the NIST made a concession and increased the maximum key length for the DSS. In regard to the patent issue, the NIST believed that the proposed DSS was not covered by any patent. The NIST addressed the fact that the DSS did not conform to international standards by stating that the DSS was intended as an alternative standard for digital signature generation and verification.[156]

2.5: State Autonomy and the Adoption of the DSS

Clearly, the NSA and the NIST exercised a great degree of autonomy in choosing the El Gamal algorithm as the basis for the algorithm in the DSS over the RSA algorithm. This event is consistent with Eric Nordlinger's Type I state autonomy, where the state is successful in implementing its policy preferences vis-à-vis powerful societal interests. In this instance, the basis of the state's policy autonomy was found in the FIPS process. This process allowed the state to set the agenda and to ultimately implement its policy preferences in regard to the government FIPS. The FIPS also provided the government agencies involved with an indirect mechanism to influence the standards used by industry since Federal Information Processing Standards were adopted by industry as well as the government. However, the indirect influence had little effect since industry had its own standard for digital signatures, the RSA algorithm. This demonstrates that the

---

[156] Approval of FIPS 186 (DSS), Electronic Privacy Information Center (EPIC), 19 May 1994, 1 Mar. 1999 <http://www.epic.org/crypto/dss/dss_approval_1994.html>.; "Digital Security Signed, Sealed, Delivered," Science News 7 Sept. 1991: 148.

agreement of all portions of the state in the United States, such as the executive, legislative, state, and local governments may not be required to exercise policy autonomy in particular areas. The El Gamal based DSA was chosen over the objections of powerful corporate interests such as Microsoft and IBM. Many persons maintain that El Gamal was chosen as the Digital Signature algorithm since it could only perform digital signatures and could not be used for encryption. However, a more plausible basis for the opposition to the El Gamal algorithm for the DSA may have been economic considerations. Bruce Schneier has argued that RSA Data Security, the large corporations that bought licenses to use RSA, and some of the experts that submitted comments had economic incentives to oppose the adoption of the proposed DSS. RSA Data Security did not want another standard competing with the RSA algorithm since this could have resulted in a loss of revenue from licensing and royalty fees. In addition, major corporations were currently using RSA products.[157] One memo from the NIST indicates that the NIST was dealing with two problems. The first was the "NSA problem" and the other was the problem over patents. The memo appears to indicate that they considered the patent problem more the serious problem at that particular time and that the issue concerning the applicability of patents over the DSS had to be resolved before the proposed DSS was released.[158] One of the intentions for the proposed DSS was that it would "be available for public use on a royalty-free

---

[157] Schneier 484.

[158] Dennis Branstad, Memorandum for Ray Kammer and Mike Rubin, 19 Oct. 1990, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

basis."[159] The NSA may have selected the El Gamal since they felt that PKP's patent claim was questionable.[160] The El Gamal algorithm had been first published in the periodical, IEEE Transactions on Information Theory in 1985.[161] Since it was first published in an academic publication, the United States government may have thought that it could be used by the public on a royalty-free basis, as opposed to RSA. However the patent issue did not appear to have been resolved when the Federal Register notice for public comment on the proposed DSS was issued on August 30, 1991. In fact, during the public comment period on the proposed DSS, the NIST received a letter from Dr. Claus Schnorr who claimed that the DSA infringed on an American patent that he owned.[162] In addition the failure to incorporate an algorithm for key exchange in the proposed DSS, such as Diffie–Hellman, could also be plausibly explained as an attempt not to subject the DSS to any royalties. The NSA does not appear to have been involved in the decision not to incorporate the Diffie-Hellman key exchange mechanism in the proposed DSS. In fact, the NSA appeared to be in favor of using the Diffie-Hellman key exchange

---

[159] A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), Electronic Privacy Information Center (EPIC), 30 Aug. 1991, 9 July 1998 <http://www.epic.org/crypto/dss/dss_fr_notice_1991.html>.

[160] Bruce Schneier has also questioned the claim that the El Gamal algorithm was covered by PKP patents. Schneier 605.

[161] John Raubitschek, memorandum for Mike Rubin, 10 June 1991, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC. Note: A study was done on the patent issues surrounding the El Gamal algorithm. However, much of the report appears to have been blanked out, due to deliberative process privilege and attorney client privilege. NSA memorandum, 11 June 1991, NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

[162] C.P. Schnorr, letter to Director, Computer Systems Laboratories, 30 Oct. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

algorithm with the El Gamal algorithm.[163] PKP's claim to hold the patent to this key exchange mechanism would have been very strong and it is unlikely that the United States government could challenge the legitimacy of the patent claim. In addition, the United States government itself was going to patent the DSA in the proposed DSS in order to make sure that no royalties would be charged for its use.[164] In the Federal Register notice announcing the adoption of the DSS, the NIST stated that the DSS was intended as an alternative to existing international standard.[165] The president of RSA Data Security, James Bidzos, appeared to notice this and offered his comments in a letter to the Chairman of the Subcommittee on Technology and Competitiveness of the House Committee on Space, Science and Technology in that regard:

> ... NIST's behavior gives every indication that they are aggressively pursuing a U.S. commercial standard based on their system, attempting to supplant existing *de facto* [sic] standards, and employing every means available to accomplish these objectives.[166]

The short-term adoption of the DSS is consistent with a high degree of state policy autonomy. The NIST and other federal agencies involved with the development of the DSS had to have known that their choice would have wider implications for industry, since these standards had broader implications beyond

---

[163] Dennis K. Branstad, memo for the record, 27 April 1990.

[164] Who Holds the Keys?,"Communications of the ACM 35.7 (1992) 54.

[165] Approval of FIPS 186 (DSS), Electronic Privacy Information Center (EPIC), 1 March 1999 <http://www.epic.org/crypto/dss/dss_approval_1994.html>.

[166] D. James Bidzos, letter to Tim Valentine, 20 Sept. 1991, Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

the United States government. However, the various parts of the American state involved in developing the DSS did not appear to exercise any significant long-term power, since adoption of DSS has been minimal. According to Bruce Schneier, the NIST was trying to facilitate the use of the DSS within the United States government. In addition, the DSS was also used by Shell Oil as their standardized digital signature method.[167] The cryptographic program Pretty Good Privacy (PGP) also uses the DSS. In regards to ANSI standards, the first standard for digital signatures was based on the DSS standard (ANSI X9.30). However, the RSA based ANSI X9.31 standard was developed to conform to the existing standards of the financial services sector.[168] RSA Data Security has also licensed its security and authentication products to many corporations worldwide.[169] The widespread licensing of RSA occurred before the proposed DSS was released for public comment. In this instance, RSA Data Security exercised structural power since it has, in large part, determined the electronic public key authentication structures, under which state and non-state actors operate. On February 3, 1999, RSA Data Security announced that the NIST was modifying the existing DSS to accept digital signatures based on the ANSI X9.31 standard.[170] As mentioned before, this

---

[167] Schneier 494.

[168] "RSA Labs FAQ – Is RSA a defacto standard?" RSA Laboratories, FAQ 4.0, RSA Data Security Inc., 21 Feb. 1999 <http://www.rsa.com/rsalabs/faq/html/3-1-11.html>.

[169] RSA Data Security- Licensee List, RSA Data Security Inc., 6 Oct. 1998 <http://www.rsa.com/html/licensees.html>.

[170] RSA Press Release – U.S. Department of Commerce Approves RSA Digital Signature Standard, RSA Data Security Inc., 3 Feb. 1999, 16 Feb. 1999 <http://www.rsa.com/pressbox/html/990203.html>.

standard allows for the generation and verification of digital signatures based on the RSA algorithm. This action could be perceived as an admission that certain United States government agencies, the NIST and NSA, were unsuccessful in displacing the dominant international RSA based standards. However, it should not be taken as a total admission of defeat for the elements of the American state involved in the development of the original DSS. There was no repudiation of the original DSA, only a modification to accept an RSA based standard.

CHAPTER THREE: AFTER THE DSS

3.1: The Escrowed Encryption Standard

The Escrowed Encryption Standard (EES) was the next and infinitely more controversial plan of certain elements of the United States government to exercise control over cryptography policy. The EES was being developed by national security agencies within the United States government in the early 1990's. In its proponent's perception, the EES and its implementation mechanism, known as the "Clipper Chip" was an attempt to reconcile the requirement for communications security and access to encrypted communication by law enforcement and national security agencies.[171] Even though the ESS and the associated "clipper chip" were to be used in United States government, their adoption in the private sector were encouraged. The "Clipper Chip" was initially intended for telephone security devices, but a chip for computers and other devices, called the "Capstone Chip" was also designed. This chip would be implemented in a computer card called "Fortezza." The Capstone Chip, unlike the clipper chip, was actually used in a number of commercial products, although no key recovery system was used. One company, Mykotronx, would manufacture the chips in a secure environment. The chip employed a classified, NSA-designed algorithm called "skipjack," and the chip was also placed in a "tamperproof" environment.[172] Like the DSS, government

---

[171] White House Clipper Statement (4/16/93), Electronic Privacy Information Center (EPIC), 16 April 1993, 11 July 1998 <http://www.epic.org/crypto/clipper/white_house_statement_4_93.html>.

[172] The EES was symmetric cryptographic system and thus required the same keys for encryption and decryption of data. Each chip would be equipped with its own key. During the manufacturing process the key would be split into two parts, for security reasons. Each part of the

agencies in the United States recruited an ally in the private sector, American Telephone and Telegraph (AT&T), to advertise the desirability of the technology. AT&T was attempting to develop a line of telephone security devices which used the DES. Security agencies convinced AT&T to use the new "clipper chip" in their new line of phone security devices. The United States government even offered to buy some of the new phone security devices to show their support of the 'clipper chip" technology. Like the DSS, the EES was instituted as a FIPS, despite a great deal of negative reaction and opposition from privacy and business interests. The United States government also tried to get other countries to endorse the proposal, but was unsuccessful.[173] Again, security and law enforcement agencies demonstrated a great deal of policy autonomy by instituting the EES as a FIPS. Like the DSS, market forces were instrumental in defeating the EES once it was adopted. The AT&T phone security devices with the clipper chip had a dismal market performance. Again, structural power over the development of electronic networks was clearly being exercised by non-state actors, such as markets, despite the great degree of policy autonomy manifested by elements of the United States government through the FIPS process and pronouncements of executive agencies.

---

key would be held by an "escrow agency." These escrow agencies were the NIST and the Automated Services Branch of the Treasury Department. Where conditions warranted, law enforcement agencies could approach the escrow agencies for the parts of a particular key. The law enforcement agency was required to present evidence that a lawful wiretap was being used and that the wiretap had been compromised due to the data being encrypted.

[173] Schneier and Banisar 307-319.

Currently, the NIST is developing the Advanced Encryption Standard (AES) as a replacement for the DES.[174] In August 1998, fifteen candidate algorithms for the AES were announced. In September 1998, the NIST requested public comment on the candidate algorithms. In the summer of 1999, at least five algorithms will be subjected to more rigorous testing, before one is selected as the AES in the early 21st century. As with the DES, the United States government intends for the AES to be used for the protection of unclassified information within the federal government and the private sector. Use of the AES will be royalty-free, and unlike the EES, the algorithm will be unclassified.[175] In contrast to the prior DSS and EES the selection process surrounding the AES appears to be very public and transparent. At the time of writing, no accusations have been made that the NSA or any other national security or law enforcement agency has tried to influence the proposed standard.

3.2: Export Controls

One area where the United States government has been successful in implementing its policy preferences in regard to encryption technologies has been export controls. It should be noted that the United States has both unilateral and

---

[174] An Electronic Frontier Foundation team successfully cracked the 56-bit DES encryption in July 1998. They constructed a machine that cracked the 56-bit DES code in 3 days for $250,000. EFF DES Cracker Project, Electronic Frontier Foundation (EFF), 17 July 1998, 6 Aug. 1998 <http://www.eff.org/descracker>.; Electric Frontier Foundation (EFF), Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design (Sebastopol: O'Reilly & Associates, 1998)

[175] NIST announces candidates for new data scrambling standard, National Institute of Standards and Technology (NIST), 20 Aug. 1998, 30 Sept. 1998 <http://www.nist.gov/public_affairs/releases/n98-15.htm>.; Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES), National Institute for Standards and Technology (NIST), 14 Sept. 1998, 2 Mar. 1999 <http://csrc.nist.gov/encryption/aes/round1/aes_9809.htm>.

multilateral export controls. The multilateral export controls have involved organizations such as the Coordinating Committee for Multilateral Export Controls (COCOM)[176] and its successor, the Wassenaar Arrangement.[177] Unilateral export controls on encryption technologies remain despite the opposition of corporations and others who would like to see them reduced or eliminated altogether. One possible explanation for the "staying power" of export controls, despite some concerted efforts to remove or reform them can be found within the American political system itself. State agencies were able to exercise autonomy in the cases of the DSS and EES since they were adopted under the FIPS process, which allowed the state to act autonomously, since state actors could control the process and the outcome. However, the FIPS process does not cover the export control legislation. It is therefore more open to normal political processes, which involve conflict and cooperation between the executive, legislature and judiciary. A possible clue to the resilience of export controls lies in one comparative examination of environmental policy. This study examined the ability of particular political system to represent diffuse political interests. One of the conclusions of the study was that the United States was able to maintain a high degree of environmental protection since there were many points of access to the American political system for diffuse interests to potentially influence the policy process. This openness made it difficult for interests that wanted to decrease environmental

---

[176] Michael Mastanduno, "The United States Defiant: Export Controls in the Postwar Era," Daedalus 120.4 (1991): 91-112

[177] History of the Wassenaar Arrangement, Wassenaar Arrangement, 29 Mar. 1999 <http://www.wassenaar.org/docs/History.html>.

protection to get their policy preferences enacted.[178] Advocates of environmental protection could exercise influence in the multitude of American political institutions. In the same way, changes to the export control regime on this type of technology may be difficult.[179] The same asset in environmental protection policy may be a liability in reform of the export controls on encryption software and hardware. National security and law enforcement interests or those politicians who are sympathetic to them may also take advantage of the many institutional opportunities to influence export control policies related to these technologies.

---

[178] David Vogel, "Representing Diffuse Interests in Environmental Policymaking," Do Institutions Matter?: Government Capabilities in the United States and Abroad eds. R. Kent Weaver and Bert A. Rockman (Washington: Brookings Institution, 1993) 237-271.

[179] This is implied in one account of cryptography policy in the United States, although not explicitly stated. Schneier and Banisar 635-670.

CHAPTER FOUR: CONCLUSION

The utility of the statist approach is demonstrated in this case study. Despite the rhetoric of state decline, this approach proved useful in understanding the dominant part played by state agencies in the adoption of the United States government's standard for digital signatures. The case of the DSS demonstrates the differing observations of Cogburn and Strange concerning state power and autonomy over telecommunications. Cogburn noticed that states were still capable of exercising considerable autonomy in regard to telecommunications policy, as demonstrated by his case study of South Africa. In the case of the DSS, executive agencies were able to exercise considerable autonomy in selecting an alternative standard for digital signatures, instead of the dominant RSA standard. State autonomy was exercised through the FIPS process, which allowed these agencies to essentially present their proposal as a "*fait accompli*" in a nearly complete form for public comment. Even though there was a great deal of opposition to the proposed DSS, it was adopted as a FIPS, with some changes, notably a longer key length. The FIPS process also allowed the United States government an indirect opportunity to influence standards used by industry, since some United States government standards, such as the DES, had been previously adopted by industry. In addition, the United States government successfully influenced the X9 committee of ANSI to adopt a standard based on the proposed DSS. Susan Strange noticed that telecommunications was one area where the decline of state power was most noticeable. The United States government was unsuccessful in getting industry to adopt its standard for digital signatures. The United States

government lacked the structural power over electronic networks necessary to influence standards used by industry. The *de facto* standard, RSA, remained the standard for digital signatures. It is clear that industry possesses the structural power, in regard to public key authentication technologies since industry has determined the technology that is to be used in this area.

The case of the DSS suggests that Scott Turner's observations concerning state/corporate relationships require some elaboration. The DSS and cryptography policy in general, suggest that the more distance there is between state and corporate interests and goals, the more conflict rather than cooperation will characterize the relationship between the two. In the case of the DSS, both state interests and some corporations, such as Microsoft, took diametrically opposed positions on the basic issue on state versus industry standards.

Application of the ACF did not work as intended. There were a number of factors, such as the limited time frame and the lack of policy-oriented learning, which limited its application and overall effectiveness. However, the application of the ACF may be considerably more difficult in some areas where there are multiple participants from other policy sub-systems. The requirement for distinct policy sub-systems may prove problematic in examining public policy related to electronic networks due to the convergence of differing policy areas, such as broadcasting, telecommunications and computing. There could be considerable difficulty in forming the organizations and individuals involved into coherent advocacy coalitions since their core and near core values could differ greatly or could be difficult to determine.

The ACF's focus on natural resources as a stable factor may also be problematic in an information society and economy. The ownership and control over natural resources may not automatically confer power on a state, as they did in the past. Other factors, such as expertise, knowledge, and capital would appear to be more important factors in an information economy than natural resources. Factors such as expertise, knowledge, and capital could also be considered dynamic factors, since sources and amounts of these factors may change, whereas the distribution of natural resources is predetermined by physical and geologic factors.

In further research on encryption standards policy, the ACF could be applied to the DES, DSS, SHS, EES, and the AES. A longer-term study could attempt to determine if the ACF could be successfully applied to policy regarding advanced electronic networks and attempt to determine whether there were actual cohesive advocacy coalitions throughout these battles over cryptographic standards.

One indicator of state autonomy in regard to the development of electronic networks is who exercises long-term power over a particular aspect of electronic networks.[180] In some cases, states and governments may mandate that certain procedures be followed or that certain technologies be employed in the development of electronic networks. Even though corporations may be

---

[180] Susan Strange noticed that "power over" was a superior conception of power than "power from." Strange The Retreat of the State, 25.

responsible for the development of all or part of an electronic infrastructure, they may not have absolute power, due to government or state interventions. One example mentioned previously was the United States government's export restrictions on cryptographic software and hardware. In the development of secure international electronic networks, the private sector must deal with the United States restrictions on the export of encryption technologies. Another indicator of state autonomy in the development of electronic networks may include the degree to which a state or government is willing to directly interfere in the development of electronic networks. In the case of the DSS and the EES, the United States government was actively involved, although it was trying to exercise power in an indirect manner through the FIPS process. Ultimately, these indirect interventions failed. The United States has also tried to directly interfere in the development of advanced electronic networks, through legislation that requires telecommunications companies to incorporate wiretapping capabilities into advanced communications networks. The degree and success of intervention by states and governments versus markets and corporations would be a prime indicator of autonomy in policy related to advanced electronic networks.

In terms of methodology, research into technical areas such as encryption and authentication will require more examination of technical literature by those engaged in research in this policy area. An examination of technical literature from disciplines such as computer science is necessary to fully understand the

technology involved and the resulting policy issues and consequences. However, technical literature may prove inadequate in answering questions and drawing conclusions about basic values of the participants involved in a particular policy area or conflict. In addition, more use and consideration must be given to electronic documents in research on advanced electronic networks. Events that impact on this policy area occur at an extremely fast rate. Electronic sources can act as documentation of the fast-paced changes in electronic networks which ultimately effect public policy. In addition, many research materials that would be ordinarily be difficult to obtain, could be procured by using electronic networks. With the wide availability of documentation, more researchers would have access to this material and more studies could be conducted on this and other issues. With the wide availability of information, more researchers with differing cultural and theoretical perspectives could conduct research, which may provide important insights into this and other policy areas.

Another methodological observation is that research on electronic networks will have to be done in a more "holistic" manner. The term "holistic" is intended to denote that perspectives from a number of other policy areas covered by advanced electronic networks will have to be used in order to examine policy regarding advanced electronic networks. This thesis drew on observations made in the literature concerning telecommunications policy, some standards literature and other areas. This "holistic" view mirrors the convergence of communications and information technologies. The changes that are occurring can only be appreciated by examining literature and theoretical observations from a number of areas.

This case study examined one particular instance in which state actors were attempting to influence policy. However, this does not mean that states cannot exert autonomy in other areas of public policy regarding electronic networks. The role of the state may increase in a number of areas. State intervention could be used to accomplish certain goals such as consumer protection. Suzanne Lütz described this in her study of stock exchange regulation in Germany. In that situation, state intervention was required in order to secure compliance to international norms. It is possible that state intervention will be necessary in order to secure compliance to regulations and legal norms in regard to advanced electronic networks. One possible area of state intervention could be the endorsement or licensing of certification authorities in order to maintain trust in a public key infrastructure. Even concerning cryptographic standards, the American state may still have some ability to indirectly influence standards. If the AES is upheld in repeated testing as being safe and trustworthy, it could become a world standard, like its predecessor the DES.

This case study examined the United States, however its conclusions could be applied to other developed countries. This does not mean that other countries could not exercise autonomy over the development of electronic networks. Some countries, where the state is considerably stronger than in the United States, such as China, would be able to exercise considerably more autonomy and power over the development of electronic networks.

REFERENCES

970825 decision. Electronic Frontier Foundation (EFF). 12 Jan. 1999 <http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/Legal/970825.decision>.

A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), Electronic Privacy Information Center (EPIC). 30 Aug. 1991. 9 July 1998 <http://www.epic.org/crypto/dss/dss_fr_notice_1991.html>.

Agre, Philip E., and Marc Rotenburg, eds. Technology and Privacy: The New Landscape. Cambridge: MIT Press, 1997.

Allen, George H. Letter to James H. Burrows. 20 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Approval of FIPS 186 (DSS). Electronic Privacy Information Center (EPIC). 19 May 1994. 1 Mar. 1999 <http://www.epic.org/crypto/dss/dss_approval_1994.html>.

Arendes, Vincent F. Letter to James H. Burrows. 18 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

AT&T Expands Availability of Internet Telephony Service. AT&T. 5 Nov. 1998. 5 Mar. 1999 <http://www.att.com/press/1198/981105.csb.html>.

Bamford, James. The Puzzle Palace: A Report on America's Most Secret Agency. Toronto: Penguin Books, 1983.

Barlow, John Perry. "Decrypting the Puzzle Palace." Communications of the ACM 35.7 (1992) 25-31.

Banking/financial Regulation. Bureau of Export Administration (BXA). 22 Sept. 1998. July 4, 1999 <http://www.bxa.doc.gov/Encryption/encbank.pdf>.

Barrett, Lawrence E. Letter to James H. Burrows. 14 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Barrow, Raymond S. Letter to James H. Burrows. 21 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Biddle, C. Bradford. "Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure." San Diego Law Review 33.3 (1996): 1143-1193.

Bidzos, D. James. Letter to Tim Valentine. 20 Sept. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Black, Andrew P. Letter to James H. Burrows. 21 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Branstad, Dennis K. Memorandum for the record. 27 Apr. 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Branstad, Dennis. Memorandum for John Lyons. 6 July 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Branstad, Dennis. Memorandum for Ray Kammer and Mike Rubin. 19 Oct. 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Broadbent, Steven W. Letter to James H. Burrows. 4 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

brooks.gif. Electronic Privacy Information Center (EPIC). 15 June 1998 <http://www.epic.org/crypto/csa/brooks.gif>.

Burnham, David. The Rise of the Computer State. New York: Random House Inc., 1983.

Burrows, James. Memorandum for Raymond Kammer. 30 May 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Canada. Information Highway Advisory Council (IHAC). Connection Community Content: The Challenge of the Information Highway. Ottawa: Industry Canada, 1995.

Caputo, Anthony A. Letter to Director, Computer Systems Laboratory. 24 Sept. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Chen, Bill. Letter to Director, Computer Systems Laboratory. 3 Mar. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce -Central Reference and Records Inspection Facility, Washington, DC.

Cogburn, Derrick L. "Globalization and State Autonomy in the Information Age: Telecommunications Sector Restructuring in South Africa." Journal of International Affairs 51.2 (1998): 583-604.

Cooper, Roger M. Letter to James Burrows. 28 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Cranford, Gerald F. Letter to James H. Burrows. 27 Nov. 1991. Recommended FIPS Digital Signature Standard, Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

David, Paul A., and Mark Shurmer. "Formal standards-setting for global telecommunications and information services: Towards an institutional regime transformation?" Telecommunications Policy 20.10 (1996): 789-815.

Deal, Harold G. Letter to F. Lynn McNulty. 17 Jan. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Demitros, Donald C. Letter to James H. Burrows. 6 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Diffie, Whitfield., and Martin Hellman. "New Directions in Cryptography." IEEE Transactions on Information Theory IT22.6 (1976): 644-654.

Diffie, Whitfield., and Susan Landau. Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge: MIT Press, 1998.

"Digital Security Signed, Sealed, Delivered." Science News 7 Sept. 1991: 148.

Drucker, Peter F. "The Global Economy and the Nation-State." Foreign Affairs 76.5 (1997): 159-171.

EFF DES Cracker Project. Electronic Frontier Foundation (EFF). 17 July 1998. 6 Aug. 1998 <http://www.eff.org/descracker>.

Electric Frontier Foundation (EFF). Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. Sebastopol: O'Reilly & Associates, 1998.

Evans, Peter. "The Eclipse of the State? Reflections on Stateness in an Era of Globalization." World Politics 50.1 (1997): 62-87.

Fall, Richard. Letter to James H. Burrows. 19 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Fischer, Addison M. Letter to James H. Burrows. 26 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Follett, Robert H. Letter to James H. Burrows. 25 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Ford, Warwick. "Digital Certificates." Scientific American Oct. 1998: 108.

Fougner, Robert B. Letter to Dennis K. Branstad. 20 April 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Froomkin, Michael. "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution." University of Pennsylvania Law Review 143.3 (1995): 709-897.

Ganley, Michael J. "Digital Signatures and Their Uses." Computers and Security 13.5 (1994): 385-391.

Gasser, Morrie. Letter to James H. Burrows. 18 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Gaugler, David L. Memorandum for James H. Burrows. 30 Oct. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Gegner, Karen E., and Stacy B. Veeder. "Standards Setting and Federal Information Policy: The Escrowed Encryption Standard (EES)." Government Information Quarterly 11.4 (1994): 403-422.

gephardt-letter-498.html. Internet Privacy Coalition. 2 April 1998. 13 Aug. 1998 <http://www.crypto.org/gephardt-letter-498.html>.

Greenlee, M. Blake. Letter to F. Lynn McNulty. 10 Jan. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Hawkins, Richard. "Standards for Communication Technologies: Negotiating Institutional Biases in Network Design." Communication by Design: The Politics of Information and Communication Technologies. Eds. Robin Mansel, and Roger Silverstone. Oxford: Oxford UP, 1996. 157-186.

Herzberg, A., and D. Naor. "Surf'N'Sign: Client Signatures on Web Documents." IBM Systems Journal 37.1 (1998): 61-71.

History of the Wassenaar Arrangement. Wassenaar Arrangement. 29 Mar. 1999 <http://www.wassenaar.org/docs/History.html>.

Housley, Russell D. Letter to James H. Burrows. 26 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Huigen, Jos. "Information and Communication Technology in the Context of Policy Networks." Technology In Society 15.3 (1993): 327-338.

inman.article. Electronic Frontier Foundation (EFF). 8 Feb. 1982. 13 Aug. 1998 <http://www.eff.org/pub/Privacy/Old/inman.article>.

Inman, B.R. "The NSA perspective on Telecommunications Protection in the Nongovernmental Sector." The Electronic Privacy Papers: Documents in the Battle for Privacy in the Age of Surveillance. Eds. Bruce Schneier and David Banisar. Toronto: John Wiley and Sons Inc., 1997. 347-355.

Inman, B.R., and Daniel F. Burton. "Technology and Competitiveness: The New Policy Frontier." Foreign Affairs 69.2 (1990): 116-134.

Introduction to Code Signing. Microsoft Corporation. 29 Oct. 1998 <http://www.microsoft.com/workshop/security/authcode/intro_authenticode.htm>.

Jenkins, H.W. Memorandum for Director NCSL. 18 Dec. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Johnson, Gerald R. Letter to John P. Murphy. 27 Oct. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Johnson-Laird, Andy. "The Anatomy of the Internet Meets the Body of the Law." University of Dayton Law Review 22.3 (1997): 467-509.

Jones, Thomas C. Letter to Miles Smid. 24 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Katzenstein, Peter J. "International relations and domestic structures: Foreign economic policies of advanced industrial states." International Organization 30.1 (1976): 1-45.

Klyza, Christopher McGrory., and Eric Mlyn. "Privileged Ideas and State Interests: Bombs, Trees, and State Autonomy." Policy Studies Journal 23.2 (1995): 203-217.

Krasner, Stephen D. "Approaches to the State: Alternative Conceptions and Historical Dynamics." Comparative Politics 16.2 (1984): 223-246.

Ledbetter, James. "TV-Web Convergence; Now? Ever?" The Industry Standard: The Newsletter of the Internet Economy 27 Jan. 1999. 29 Jan. 1999 <http://www.thestandard.net/articles/article_print/0,1454,3298,00.html>.

Leiner, Barry M., et al., Internet Society (ISOC) All About the Internet: A Brief History of the Internet. Internet Society (ISOC). 27 Feb. 1999 <http://www.isoc.org/internet/history/brief.html>.

Lenk, Klaus. "The challenge of cyberspatial forms of human interaction to territorial governance and policing." The Governance of Cyberspace: Politics Technology and Global Restructuring. Ed. Brian D. Loader. New York: Routledge, 1997. 126-135.

Liggett, Trish. Letter to James H. Burrows. 22 Nov 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Lütz, Susanne. "The revival of the nation-state? Stock exchange regulation in an era of globalized financial markets." Journal of European Public Policy 5:1 (1998): 153-168.

Mann, Michael. "Has globalization ended the rise and rise of the nation-state?" Review of International Political Economy 4.3 (1997): 472-496.

Martin, Cathie Jo. "Business Influence and State Power: The Case of U.S. Corporate Tax Policy," Politics & Society 17.2 (1989): 189-223.

Mastanduno, Michael. "The United States Defiant: Export Controls in the Postwar Era." Daedalus 120.4 (1991): 91-112

McCullagh, Declan. "Landmark Ruling on Encryption." Wired News 6 May, 1999 <http://www.wired.com/news/news/politics/story/19553.html>.

McNulty, F. Lynn., and Dennis K. Branstad. Memorandum for Raymond G. Kammer. 21 Nov. 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Memorandum for the record. 13 March 1991. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Myhrvold, Nathan P. Letter to James H. Burrows. 21 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Mitchell, Jeremy. "Convergent Communications, Fragmented Regulation and Consumer Needs." Telecom Reform: Principles, Policies and Regulatory Practices. Ed. William H. Melody. Lyngby: Technical University of Denmark, 1997. 441-451.

Nelson, Kristine M. "The Clipper Initiative: Fact or Fiction in Future Encryption Policy." Hamline Journal of Public Law and Policy 16.1 (1994): 291-311.

Network Associates Announces Availability of 128bit PGP Encryption Software for Global Customers. Network Associates Incorporated (NAI). 20 Mar. 1998. 13 Aug. 1998 <http://www.nai.com/about/news/press/1998/march/032098.asp>.

NIST announces candidates for new data scrambling standard. National Institute of Standards and Technology (NIST), 20 Aug. 1998. 30 Sept. 1998 <http://www.nist.gov/public_affairs/releases/n98-15.htm>.

NSA Memorandum. 11 June 1991. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

O'Sullivan, Patrick B. "Computer Networks and Political Participation: Santa Monica's Teledemocracy Project." Journal of Applied Communication Research 23.2 (1995): 93-107.

Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy. Global Information Infrastructure – Global Information Society (GII-GIS): Policy Requirements. Paris: OECD, 1997. 5 Feb. 1999 <http://www.oecd.org/dsti/sti/it/infosec/prod/e_97-139.pdf>.

Organization for Economic Co-operation and Development (OECD). Committee for Information, Computer and Communications Policy. Group of Experts on Information security and Privacy. Inventory of Approaches to Authentication and Certification in a Global Networked Society. 16 Oct. 1998 <http://www.ottawaoecdconference.org/english/announcements/reg3r3e.pdf>.

Owens, John F. Memorandum to James H. Burrows. 1 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Panitch, Leo. "The Role and Nature of the Canadian State." The Canadian State: Political Economy and Political Power. Ed. Leo Panitch. Toronto: UT Press, 1987. 3-27.

Pasquariello, C.J. Letter to James H. Burrows. 28 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Perl, Anthony. "Public Enterprise as an Expression of Sovereignty: Reconsidering the Origin of Canadian National Railways." Canadian Journal of Political Science 27.1 (1994): 23-52.

Petrie, Lorraine. Letter to James H. Burrows. 20 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Phillips, Reed. Memorandum for James H. Burrows. 27 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Priven, Lew. Letter to James Burrows. 25 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Randolph, Lynwood P. Letter to James H. Burrows. 18 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Rattray, Greg. "The Emerging Global Information Infrastructure and National Security." Fletcher Forum of World Affairs 21.2 (1997): 81-99.

Raubitschek, John. Memorandum for Mike Rubin. 10 June 1991. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS), EPIC, Washington, DC.

Reddin, Thomas E. Memorandum to Director, Office of Organization and Management Systems- Public Health Service. 20 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES). National Institute for Standards and Technology (NIST). 14 Sept. 1998. 2 Mar. 1999 <http://csrc.nist.gov/encryption/aes/round1/aes_9809.htm>.

Replay Associates. Replay Associates L.L.P. 21 March 1999 <http://www.replay.com>.

Rhodes, Marc. Letter to James H. Burrows. 27 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Rotenberg, Marc., and David Sobel. Letter to Director, Computer Systems Laboratory. 24 Oct. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

RSA Data Security- Licensee List. RSA Data Security Inc. 6 Oct. 1998 <http://www.rsa.com/html/licensees.html>.

"RSA Labs FAQ – Can RSA be exported from the United States?" RSA Laboratories. FAQ 4.0. RSA Data Security Inc. 3 March 1999 <http://www.rsa.com/rsalabs/faq/html/6-4-1.html>.

"RSA Labs FAQ – Is RSA a defacto standard?" RSA Laboratories. FAQ 4.0. RSA Data Security Inc. 21 Feb. 1999 <http://www.rsa.com/rsalabs/faq/html/3-1-11.html>.

"RSA Labs FAQ – What are ANSI X9 Standards?" RSA Laboratories. FAQ 4.0. RSA Data Security Inc. 21 Feb. 1999 <http://www.rsa.com/rsalabs/faq/html/5-3-1.html>.

"RSA Labs FAQ – What is RSA?" RSA Laboratories. FAQ 4.0. RSA Data Security Inc. 3 March 1999 <http://www.rsa.com/rsalabs/faq/html/3-1-1.html>.

RSA Press Release – U.S. Department of Commerce Approves RSA Digital Signature Standard. RSA Data Security Inc. 3 Feb. 1999. 16 Feb. 1999 <http://www.rsa.com/pressbox/html/990203.html>.

Sabatier, Paul A. "Policy Change over a Decade or More." Policy Change and Learning: An Advocacy Coalition Approach. Eds. Paul A. Sabatier, and Hank C. Jenkins-Smith. Boulder: Westview Press. 1993. 13-39.

Sattler, Michael. Letter to James H. Burrows. 11 Dec. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Schlafly, Roger. Letter to NIST. 11 Oct. 1990. NSA/NIST Documents Concerning the Development of the Digital Signature Standard (DSS). EPIC, Washington, DC.

Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. Toronto: John Wiley and Sons, 1996.

Schneier, Bruce., and David Banisar, eds. The Electronic Privacy Papers: Documents in the Battle for Privacy in the Age of Surveillance. Toronto: John Wiley and Sons Inc, 1997.

Schnorr, C.P. Letter to Director, Computer Systems Laboratories. 30 Oct. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Schwartz, Michael. Letter to Director, Computer Systems Laboratory. 12 Sept. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Sematech Events: 1995. Sematech. 1 Feb. 1999 <http://www.sematech.org/public/general/timeline/95.htm>.

Shine, Kenneth I. "Impact of Information Technology on Medicine." Technology In Society 18.2 (1996): 117-126.

Sims, Fred L. Letter to James H. Burrows. date obscured. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Skocpol, Theda. "Bringing the State Back In: Strategies of Anaylsis in Current Research." Bringing the State Back In. Eds. Peter B. Evans, Dietrich Rueschemeyer, and Theda Skocpol. Cambridge: Cambrige UP, 1985. 3-37.

Sobel, David L. "Government Restrictions on the Development and Dissemination of Cryptographic Technologies: The Controversy over the Digital Signature Standard," Computer Law Reporter 16.256 (1992): 265-270.

Sobel, David L. New NIST/NSA Revelations. Electronic Privacy Information Center (EPIC). 22 July 1998 <http://www.epic.org/crypto/dss/new_nist_nsa_revelations.html>.

Spencer, Doris J. Letter to James H. Burrows. 29 Jan. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Stamper, Chris. "Guilty Verdict for Cypherpunk." Wired News 20 Apr. 1999 <http://www.wired.com/news/print_version/politics/story/19239.html?wnpg=all>.

Stipp, David. "11.11.96 TECHNO HERO OR PUBLIC ENEMY?" Fortune 11 Nov. 1996. 7 Oct. 1998 <http://pathfinder.com/@@qPRqOwYA60VQwxah/fortune/1996/961111/rsa.htm>.

Strange, Susan. States and Markets. 2nd ed. London: Pinter, 1994.

Strange, Susan. "The Defective State." Daedalus 124.2 (1995): 55-74.

Strange, Susan. The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge: Cambridge UP, 1996.

Stritch, Andrew J. "State Autonomy and Societal Pressure: The Steel Industry and U.S. Import Policy." Administration and Society 23.3 (1991): 288-309.

Stupack, Ronald J., and Thomas C. Hone. "National Security and Domestic Policy Making: The Similarities and the Critical Differences." International Journal of Public Administration 15.7 (1992): 1441-1447.

Turner, Scott. "Transnational Corporations and the Question of Sovereignty: An Alternative Theoretical Framework For the Information Age," Southeastern Political Review 25.2 (1997): 303-324.

Tyler, Michael. Briefing Report on Transforming Economic Relationships in International Telecommunications. Geneva: ITU, 1998.

United States. General Accounting Office (GAO). Communications Privacy: Federal Policy and Actions. Washington: General Accounting Office, 1993.

---. General Accounting Office (GAO). Information Superhighway: An Overview of Technology Challenges. Washington DC.: General Accounting Office, 1995.

Vogel, David. "Representing Diffuse Interests in Environmental Policymaking." Do Institutions Matter?: Government Capabilities in the United States and Abroad. Eds. R. Kent Weaver, and Bert A. Rockman. Washington: Brookings Institution, 1993. 237-271.

Waldron, Miles D. Letter to James H. Burrows. 20 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Welcome to DENradio.com. Interactive Netcasting Systems Inc. 21 March 1999 <http://www.denradio.com/index.shtml>.

Welcome to DENtv.com. Interactive Netcasting Systems Inc. 21 March 1999 <http://www.dentv.com/index.shtml>.

White House Clipper Statement (4/16/93). Electronic Privacy Information Center (EPIC). 16 April 1993. 11 July 1998 <http://www.epic.org/crypto/clipper/white_house_statement_4_93.html>.

"Who Holds the Keys?" Communications of the ACM 35.7 (1992): 53-54.

Wood, Joseph J. Letter to James H. Burrows. 20 Feb. 1992. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Zimmerman, Dale G. Letter to James H. Burrows. 8 Nov. 1991. Recommended FIPS Digital Signature Standard. Department of Commerce-Central Reference and Records Inspection Facility, Washington, DC.

Zimmerman, Philip R. "Cryptography for the Internet." Scientific American Oct. 1998: 110-115.