From Clipper to Carnivore:
Balancing Privacy, Law Enforcement and Industry Interests

Priscilla M. Regan
Department of Public and International Affairs
George Mason University
pregan@gmu.edu

July 2001

Prepared for delivery at the 2001 Annual Meeting of the American Political Science Association, San Francisco, CA, August 29-September 2, 2001.

From Clipper to Carnivore:
Balancing Privacy, Law Enforcement and Industry Interests

Abstract

Law enforcement officials value their ability and legal authority to monitor the flow of communications and to intercept the content of messages. Title III of the 1968 Omnibus Crime Control and Safe Streets Act establishes the legal framework for standards and procedures to obtain court ordered wiretaps. But new communications channels, such as the Internet, and sophisticated encryption technologies challenge law enforcement's ability to monitor communication flows and to understand messages. In 1993 the Clinton administration proposed an encryption scheme involving the Clipper Chip, which would employ key-escrow technology and involve two government agencies holding the keys for decoding messages. In 2000 the Clinton administration proposed Carnivore, which would be installed at the facilities of Internet Service Providers to monitor Internet traffic. This paper analyzes the interplay among privacy, law enforcement and communication industry interests in policy debates regarding wiretapping and encryption. The paper pays particular attention to the role and influence of industry interests. In previous decades, similar debates were framed as a conflict between law enforcement and civil liberties with the balance generally tipping in favor of law enforcement. The paper examines how the entry of the communications industry into the more recent debates affects the dynamics of policymaking, the discourse about ideas and interests, and policy outcomes.

Introduction

On April 16, 1993 the Clinton administration announced an encryption initiative that it depicted as bringing "the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement."[1] This announcement provoked what would become a seven-year debate between law enforcement and national security, on the one side, and industry and privacy advocates, on the other. The initiative involved the development of a key-escrow system whereby devices containing the Clipper Chip could encrypt or code messages and would have two keys each of which would be deposited in a separate government database. Decoding the message would require access to both keys. Government officials would only be able to access the keys with a court order. The White House viewed the Clipper Chip as a way of providing law-abiding citizens with encryption technology and preventing criminals from hiding illegal activities.

Although this initiative might appear consistent with a long tradition of balancing law enforcement and civil liberties interests, the process by which it was developed and the substance of the proposal itself were fraught with difficulties. The Clipper Chip was

[1] The White House, Office of the Press Secretary, *Announcement of the Clipper Chip Encryption Technology* (April 16, 1993). Available at: http://www.cdt.org/crypto/admin/041693whpress.txt

developed with active involvement by the National Security Agency, an organization whose jurisdiction did not include domestic encryption and whose deliberations were closed to the public. The White House viewed this announcement as the beginning of public debate and consultations with industry, but many were skeptical about such intentions given the administration's commitment to the initiative.[2] Regardless of the process by which it was developed, many computer specialists questioned its effectiveness, privacy advocates doubted the wisdom of having keys held by government agencies, civil liberty groups raised First, Fourth and Fifth Amendment concerns, and industry representatives queried the impact this would have on their position in the global marketplace.

Within a few weeks of the announcement of the Clipper Chip, a letter questioning the plan and requesting more extensive public discussion was sent to President Clinton. The letter was circulated by the Electronic Frontier Foundation (EFF), a public interest group, and signed by more than 30 technology companies, including IBM, AT&T, Lotus, Microsoft and MCI, trade associations, and advocacy groups, including the ACLU.[3] A month later, at a cryptography and privacy conference organized by Computer Professionals for Social Responsibility (CPSR), the acting director of the National Institute of Standards and Technology (NIST) announced, consistent with the recommendation of its own advisory panel on privacy, that plans for the Clipper Chip would be slowed for further study and deliberation.[4]

The Clipper Chip proposal sparked a seven year debate that resulted in no legislation despite numerous hearings and bills, two major court challenges, and an administrative retreat from its original proposal to an acceptance of the policy position advanced by business, privacy advocates and policy experts. But as the Clipper Chip chapter ended, the Carnivore proposal provoked a similar conflict between law enforcement and national security on the one hand and industry and privacy advocates on the other.

The purpose of this paper is not to advocate or evaluate a policy stance, but to analyze the process by which policy is being formulated. Some cyberspace commentators argue that cyberspace is an inherently new and different milieu in which traditional laws, values, and institutions have no place. Other pundits suggest that cyberspace will fundamentally alter governments and politics. Few, if any, commentators take the position that "politics as usual" will dominate policymaking for cyberspace issues. It is not surprising that observers of online policy issues would be attuned to the unusual and unique, and would emphasize the challenges in governing cyberspace. But the reality is that a number of online policy issues are being addressed

---

[2] As part of the announcement, the President approved a Presidential Decision Directive on "Public encryption Management" that instructed the Attorney General to request manufacturers of communications hardware to install US government-developed key-escrow microcircuits and to make arrangements to hold the keys for key-escrow microcircuits, and directed the Secretary of Commerce to begin developing standards for procurement and use of encryption devices.

[3] John Burgess, "Encryption Decision is Questioned," *The Washington Post* (May 7, 1993), p.F3.

[4] John Schwartz, "U.S. Data Decoding Plan Delayed; Business and Legal Objections Reviewed," *The Washington Post* (June 8, 1993), p.A12

through the normal American political processes with separate institutions sharing power and providing access points for a host of interested parties.

This paper seeks to empirically explore how these processes are working through an examination of the policy processes associated with encryption and online wiretapping. Are online policy questions evoking a unique form of politics or are the policy questions familiar enough to elicit "politics as usual"? Are questions about the role of government in cyberspace fundamentally distinct from previous questions about the role of government? Are there new actors or players in cyberspace and do they have different interests and ideas? Is there a different constellation of government institutions that become involved and are their activities altered? An organizational trilogy of ideas, interests and institutions will be employed for purposes of analyzing the politics of online privacy. The discussion will evaluate whether the political circumstances of cyberspace reflect fundamentally new characteristics or ones that are quite typical of American politics.

Ideas

Throughout the policy discussions regarding both the Clipper Chip and Carnivore, five ideas dominated policy discourse and provided the rationale for the arguments that interest groups, administration officials and members of Congress forwarded in policy debates.

Security

Many articles about encryption and wiretapping begin by pointing out that this has traditionally been the exclusive dominion of law enforcement and national security. Coding and breaking messages sent by spies or organized crime have long been techniques that were of interest to a relatively narrow community and whose use was shrouded in secrecy.[5] Cryptographers and later computer scientists developed complex mathematical algorithms by which plain text information or bits and bytes of digitized information were converted into in effect gibberish and then sent to a receiver who had the code to reconvert the message into its original form. This protected the content of the message during transmission.

Security communications have long been a priority of the national security community and much of the work that has been done on developing encryption has been funded by or developed by national security or military agencies. Many businesses and individuals protect the security of their communications by using encryption software, such as Pretty Good Privacy, or devices with encryption. As businesses and individuals relied more and more on electronic communications, especially over the Internet, to conduct their financial, personnel, and health transactions, the importance of secure communications and the use of encryption expanded from the national security community to the general population. But at the same time the national security

[5] Frank J. Donner, *The Age of Surveillance: The Aims and Methods of America's Intelligence System* (New York: Alfred A. Knopf, 1980).

orientation was quite entrenched as reflected in the fact that encryption technologies, products and related technical information were classified by the State Department as "munitions" whose export was restricted and required a license from the Bureau of Export Administration (BXA).

Privacy

The protection of privacy in the realm of communications, especially telephone and other electronic forms, is based largely in the Constitution. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, particularly describing the place to be searched and the persons or things to be seized." This constitutional protection has been reinforced by the Supreme Court, most notably in *Katz v. United States*[6], and by Congress, most comprehensively in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act of 1986 (ECPA), and the Foreign Intelligence Surveillance Act of 1988 (FISA). These protections have come to mean that law enforcement and intelligence officials cannot surreptitiously eavesdrop on the content of electronic communications without getting a court order or access the transaction information associated with an electronic communication without official approval. They also make it illegal for private parties to intercept electronic communications.

Once people and organizations began to use encryption to secure their communications, they also enhanced the privacy of those communications because they themselves had control over who had access to the contents of communications. But encryption raised debate about whether this was more privacy than people were entitled to under the Fourth Amendment. Law enforcement officials feared that a court order would provide access to encrypted communications that they would not be able to decrypt. A key escrow system, such as the Clipper Chip, would provide law enforcement access to the keys to decrypt such messages. Privacy advocates argued that once the keys were revealed to law enforcement officials, the privacy of all communications encrypted with that key could be compromised.

Proponents of the use of encryption also argued that the Fifth Amendment protection against self-incrimination insulates users of encryption from being forced to reveal the code they were using.

Free Speech

The First Amendment prohibits the government in general from regulating the content of communications. Civil liberties groups argued that encryption was akin to use of a foreign language and that regulating or banning encryption would be similar to banning the use of a particular language, which would probably violate the First Amendment. The First Amendment does permit "time, place and manner" restrictions on

[6] 389 U.S. 347 (1967).

speech but the restrictions must be narrowly tailored and use the "least restrictive means" of achieving the government's goal. A justification for prohibiting encryption or requiring the use of a specified encryption scheme would have to meet these tests to withstand a First Amendment challenge.

Finally, the First Amendment protects freedom of expression and the exchange of ideas. Any regulation on discussion about encryption or disclosures of encryption algorithms might be considered a "prior restraint" on speech if it was agreed that these involved expressive content. The State Department's restrictions on the export of encryption technologies and information were interpreted by some as a "prior restraint."

Accountability, Openness and Trust

There is always something of a tension between a democratic political system and the police and national security functions of a state. In the United States, procedural and structural requirements for accountability and openness have been the major means by which these functions are contained. The process by which police and national security activities are carried out and developed is critical to their political acceptability. Secrecy always raises red flags. If the FBI and NSA can document that a system has been developed so that it does what it is supposed to do effectively and does only what it is supposed to do, then civil liberty concerns are mitigated. But if there has been no peer review or outside review, then the possibility of systems taking on "Big Brother" characteristics is palpable.

The natural skepticism that a democratic system brings to law enforcement and national security can be alleviated by the track record of those agencies. If agencies have carried out their functions in a responsible and constrained manner, then trust is won. If not skepticism is hard to overcome. And once trust has been broken, it is difficulty to rebuild.

Interests

In the interest model of politics, policymaking is often viewed as a process of bargaining, negotiation, and compromise among competing groups whose material interests are likely to be affected by the policy under debate. The focus here, as distinct from the focus on ideas above, is on perceptions of how particular interests will be affected by a policy problem or policy alternative. It is at this level, that interests – which may well be buttressed by ideas – come into play.

Constellation of Stakeholders

Beginning in the 1980s with the explosion of new communications technologies and media, privacy advocates, civil liberties groups and businesses recognized that they had shared concerns in the privacy and security of communications. Privacy advocates were concerned that individuals have knowledge and control over when communications

and information were being captured, retained and disclosed. Civil liberties groups were apprehensive about government access to information and communications. And businesses, as both producers of communication technologies and proprietors of information, sought to please their consumers and restrict regulation. An ad hoc coalition of privacy advocates, civil liberties groups and business worked together successfully for passage of the Electronic Communication Privacy Act in 1986.[7]

As communication policy issues raised similar concerns about privacy and security, this ad hoc coalition became somewhat formalized. The Digital Privacy and Security Working Group (DPSWG) began to work together on communications privacy issues in 1991. This coalition was coordinated primarily by the Electronic Frontier Foundation (EFF), an involved over fifty computer, communications and public interest organizations including, for example, AT&T, the United States Telephone Association, and the ACLU. The controversies over both the Clipper and the Digital Telephony Act were natural issues for this coalition.

In March 1998, a group of high technology companies and associations formed a new coalition, the Americans for Computer Privacy (ACP). By August 1998 its members included 40 associations, 90 companies, and 2,000 individuals and it had more than $5 million in funding, primarily from the largest companies such as Intel, Microsoft and Cisco Systems. Its strategy was to appeal to the public through print and broadcast advertising campaign. Its goal was to broaden interest in computer privacy and frame the issue as more than a computer issue, emphasizing instead the need to protect privacy, keep online medical and financial transactions secure, and help keep US companies competitive. This bipartisan group was headed by Ed Gillespie, president of Policy Impact Communications and a Republican insider,[8] and its general counsel was a Democratic insider, Jack Quinn a partner in Arnold and Porter.

Ability to Conduct Investigations

Law enforcement argued that the new communications technologies, both in terms of network configuration and also in terms of use of encryption, made it difficult for them to conduct investigations that would normally be permitted under the Fourth Amendment. In their analysis, new technological capabilities had tipped the balance between law enforcement and privacy in favor of privacy. At congressional hearings and press briefings, the recurring theme of law enforcement was that these capabilities hampered their ability to investigate child pornographers, drug dealers, terrorists, and other criminal forces. These statement of a special agent of the FBI before a House Subcommittee is representative:

[7] Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (Chapel Hill, NC: University of North Carolina Press, 1995), Chapter 5 and Priscilla M. Regan, "Ideas or Interests: Privacy in Electronic Communications," *Policy Studies Journal* 21, no. 3(Autumn, 1993), pp. 450-69.

[8] Elizabeth Corcoran, "Ads to Target Encryption Curbs; Group Opposes restrictions on Data-Scrambling Technology," *The Washington Post* (March 4, 1998), p. C15

> Without law enforcement's ability to effectively execute court orders for electronic surveillance, the country would be unable to protect itself against foreign threats, terrorism, espionage, violent crime, drug trafficking, kidnapping, and other crimes. We may be unable to intercept a terrorist before he sets off a devastating bomb; unable to thwart a foreign spy before he can steal secrets that endanger the entire country; and unable to arrest drug traffickers smuggling in huge amounts of drugs that will cause widespread violence and death.[9]

Although law enforcement emphasized the "immense value" of wiretapping, civil liberties groups and privacy advocates questioned that value seeking more concrete evidence of its widespread value. If wiretapping was of less value in investigations, then the law enforcement argument for its need to decrypt communications was less compelling.

Effectiveness

Related to this interest in the ability to conduct investigations was a question about the effectiveness of both the Clipper Chip and Carnivore to do what they were portrayed to do. Key escrow and key recovery encryption systems required that keys be held by or available to a third party. Several computer specialists[10] argued that this was an inherent security weakness in the system as it raised the possibility of an "insider threat" within the third party organization. There were also questions about the administrative infrastructure of "trusted third parties" and "certification agents" that would be required to operate a key escrow or recovery system.[11] Finally, there was concern that a key recovery or escrow system would not be technologically robust and inhibit an individual or organization's ability to upgrade as the technology changed.

The effectiveness of Carnivore was also questioned. According to the FBI, Carnivore was a "diagnostic tool" designed to sort through all the traffic through an Internet service provider (ISP) and to separate out only those e-mails specifically under investigation. The FBI described this as a "surgical ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept."[12] The FBI also posted on its website a diagram showing how Carnivore taps into the segment of ISP traffic believed to

---

[9] Statement of James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, Federal Bureau of Investigations, *Hearings on Security Issues in Computers and Communications*, Subcommittee on Technology, Environment and Aviation of the House Committee on Science, Space, and Technology, May 3, 1994.

[10] An ad hoc group of eminent cryptographers and computer scientists wrote two editions of a report that received much attention: Hal Abelson, et. al, *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption* (1997 &1998). Available at: http://www.cdt.org/crypto/risks98.htm

[11] Michael Froomkin, "The Essential Role of Trusted Third Parties in electronic Commerce," 75 *Oregon Law Review* 49 (1996). Available at: http://personal.law.miami.edu/~froomkin/articles/trustedno.htm

[12] Donald M. Kerr, *Internet and Data Interception Capabilities developed by the FBI*, Statement for the Record, U.S. House of Representatives, Committee on the Judiciary, Subcommittee on the Constitution, July 24, 2000. Available at: http://www.fbi.gov/programs/carnivore/carnivore.htm

contain the suspect's communications, copies all the traffic accessed at that point, filters the copied traffic to separate out the e-mails authorized by the court order and tosses all other traffic.[13] In terms of effectiveness, questions were raised about how much Internet traffic was actually siphoned off, what assurances there were that traffic not authorized by the investigation was destroyed, and how the filter was programmed.

"Genie out of Bottle"

Producers of encryption devices and software, as well as companies and organizations who wanted to buy the best encryption available, raised concerns that many encryption devices and software that were being denied export licenses by the BXA were commercially available in other countries. This was often referred to as the "genie is already out of the bottle" and attempts to put it back in will be futile and will hamper the competitiveness of American firms. This interest in global competitiveness was shared by those firms that were in the business of developing and selling encryption, as well as by those that were using encryption to secure their online personnel, proprietary and financial transactions.

Interplay Among Institutions

Clipper I

As those opposed to the Clipper Chip marshaled their resources and arguments, the Administration moved to implement its plan. In September 1993, the Department of Commerce released a draft Federal Information Processing Standard (FIPS) for key-escrow encryption standards that despite opposition from the Electronic Frontier Foundation and others was approved as FIPS 185. The Administration also announced that NIST and a non-law enforcement section of the Treasury Department would be the two escrow agents. Industry and public interest groups were critical of having two government agencies serve as escrow agents, and were concerned with the impact such a choice would have on the market for encryption.[14] Although the Administration had indicated that it would release a policy analysis of the Clipper Chip proposal as a basis for public debate, such an analysis was not produced in the time promised.[15] In response to criticisms of the clandestine manner in which policy was being developed, Stewart Baker, chief counsel for the NSA, conceded that had "some force in April of 1993," but that since that time there had been opportunities for public and industry comment. He argued that "after all this consultation, the government went forward with key

[13] FBI, *Carnivore: Diagnostic Tool*. Large Chart available at: http://www.fbi.gov/hq/lab/carnivore/carnlrgmap.htm

[14] John Mintz and John Schwartz, "Encryption Program Draws Fresh Attacks," *The Washington Post* (Sept. 18, 1993), p.C1.

[15] Jerry J. Berman, Executive Director of Electronic Frontier Foundation, *Hearing on Communications and Computer Surveillance, Privacy and Security*, Committee on Science, Space and Technology, Subcommittee on Technology, Environment and Aviation, U.S. House of Representatives, May 3, 1994. Available at: http://www.eff.org/pub/Privacy/Clipper/berman_eff_clip-dt.testimony

escrow…because none of the proposal's critics was able to suggest a better way to accommodate society's interests in both privacy and law enforcement."[16]

In early 1994, after a nine-month review, the Clinton Administration decided to continue to encourage the use of the Clipper Chip and to maintain restrictions on export of encryption devices. This position was advocated by law enforcement and national security interests, and criticized by technology companies and civil liberties groups. In response CPSR circulated an electronic petition to President Clinton urging that the Clipper Chip be withdrawn because "privacy protection will be diminished, innovation will be slowed, government accountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be threatened."[17] Within a week the petition secured over 8,000 signers. As opposition grew, some divisions within the Clinton administration emerged. At a meeting of the National Information Infrastructure Advisory Committee, Vice President Gore stated that the plans were not final especially as to who should hold the escrow keys.[18] In general, technology industry executives found Clinton's support for the National Information Infrastructure and his support for Clipper somewhat incongruous and believed that it was accounted for by Clinton's political vulnerability on national security issues.[19]

Opposition to the Clipper Chip and press attention for the issue grew during the Spring of 1994. At the March Computers, Freedom and Privacy conference, high-tech and civil liberties groups gave a "hostile reaction" to administration officials.[20] In May 1994, subcommittees of the Senate Judiciary Committee and the House Committee on Science, Space and Technology held hearings on the Clipper Chip and on the Clinton administration's proposed Digital Telephony and Communications Privacy Improvement Act of 1994, which would require all common carriers to construct their networks to allow law enforcement agencies a back door to the contents of all communications and the transactional information about those communications in real time. A similar proposal had been circulated during the Bush administration and had met with resistance from both industry and civil liberties groups. At these hearings, support for Clipper and for the Digital Telephony Bill was voiced by the Department of Justice, the National Security Agency, and Dorothy Denning, a computer science professor at Georgetown University. Opposing these initiatives were EFF, DPSWG, Stephen Walker who was president of Trusted Systems, Inc., and Whitfield Diffie, an engineer and cryptographer at Sun Microsystems.

Despite this opposition the FBI continued to argue that it faced technical barriers to wiretapping due to the use of new digital technologies. In October 1994, Congress

---

[16] Stewart A. Baker, "Don't Worry Be Happy: Why Clipper is Good for You," *Wired 2.06* (May 1994). Available at: http://www.eff.org/pub/Privacy/Clipper/clipper_good_nsa.article

[17] Computer Professionals for Social Responsibility, *Electronic Petition to Oppose Clipper* (Feb. 1994). Available at: http://www.eff.org/pub/Privacy/Clipper/clipper_cpsr.petition

[18] John Schwartz and John Mintz, "Gore: Federal Encryption Plans Flexible; High-Tech Industry Opposed to Proposal," *The Washington Post* (Feb. 12, 1994), p.C1.

[19] John Mintz and John Schwartz, "Clinton Backs Security Agencies on Computer Eavesdropping," *the Washington Post* (Feb. 5, 1994), p.A1.

[20] Michael Dresser, "High-tech advocates leery of Clipper," *The Baltimore Sun* (March 25, 1994), p.13C.

passed the Communications Assistance for Law Enforcement Act (CALEA), a revision of the Digital Telephony bill. CALEA required that telecommunications networks deployed after January 1, 1995 had to be configured to allow law enforcement wiretapping and authorized $500 million to cover the costs of modifying the network.

Clipper II

In September 1995 the Clinton Administration announced a relaxation of export controls up to 64-bit encryption keys if the encryption keys were escrowed with an agent that was certified by the government. Both industry and civil liberties groups were critical of the proposal because it was not voluntary, the up-to-64-bit key length was not regarded as secure, there were no privacy and Fourth Amendment protections, and it was not likely to be accepted globally. Three months later the Administration amended the proposal to permit the export of 64-bit encryption keys but still required key escrow.

In 1993 Congress had authorized the National Research Council (NRC) to conduct an independent study of national encryption policy including the national security, commercial and privacy interests.[21] The chair of the committee concluded that there was a "policy crisis" in that the processes of our democratic government were "unable to develop a consensus behind a coherent national cryptography policy."[22] The May 1996 report recognized that public debate had been largely framed in terms of the "privacy of individuals and businesses against the needs of national security and law enforcement" and that this "dichotomy is misleading."[23] Instead, the committee argued that both interests were legitimate. Among its most important conclusions were that: the debate about encryption could be conducted on an unclassified basis; the advantages of more widespread use of cryptography outweighed the disadvantages; there should be no ban on the manufacture, sale or use of encryption within the United States; and, export controls should be relaxed but not entirely eliminated.[24] In general, the NRC report was seen as a serious criticism of the direction of the Clinton administration's policy.

Clipper III (Summer 1996)

Even before the NRC report was released, members of Congress introduced legislation seeking a more liberal approach than advanced by the administration. Senator Leahy's Encrypted Communications Privacy Act (S. 1587) relaxed export controls, permitted the use of encryption domestically, and created a legal framework for escrow agents. Senator Conrad Burns (R-MT) introduced the Promotion of Commerce Online in the Digital Era (PRO-CODE) Act (S. 1726) which prohibited mandatory key escrow, liberalized export regulations, and permitted the sale and use of any encryption

[21] Public Law 103-160, Defense Authorization Bill for Fiscal Year 1994, signed November 30, 1993.
[22] Kenneth W. Dam and Herbert s. Lin, *Cryptography's Role in Securing the Information Society* Washington, D.C.: National Academy Press, 1996., p. xvi.
[23] Ibid., p. 3.
[24] Ibid., pp. 4-8.

domestically. Similar legislation, the Security and Freedom through Encryption (SAFE) Act (HR 3011) was introduced in the House by Representative Bob Goodlatte (R-VA).

In June and July 1996, a subcommittee of the Senate Commerce, Science and Transportation Committee held hearings on encryption legislation especially S. 1726, the Promotion of Commerce On-Line in the Digital Era (Pro-Code) Act. Concerns expressed at the June hearings mirrored those of earlier hearings and debates.[25] The issue of the loss of market share to American software and computer companies was raised by a number of witnesses. Philip Karn, a staff engineer for Qualcom, Inc., described how export controls and bureaucratic delays hampered Qualcom's ability to sell and supports its products overseas. Senator Ashcroft (R-MO) also questioned the logic of a scheme that permitted American companies to sell encryption products to American users, but not to anyone else although the same products are available worldwide by other companies in other countries. Whitfield Diffie drew a comparison between the global market effects of export restrictions on the computer and software industry to the loss of market share experienced by American television set manufacturers in their competition with the Japanese. The question of the effectiveness of a key escrow scheme was raised by several witnesses and by Representative Bob Goodlatte who had introduced similar legislation in the House.

At the July hearings, the key focus continued to be on balancing law enforcement and national security concerns against economic concerns about U.S. competitiveness. At this time, the Bureau of Export Administration, in part as a result of a study it conducted with the National Security Agency, recommended that the government step back from assuming a controlling role in a key escrow scheme and instead allow industry to develop and implement a key management infrastructure which would permit government to recover a key when necessary. As described by William Reinsch, the Undersecretary for Export Administration in the Department of Commerce, the role of the federal government would be to work "with industry to set standards for federal use of these products, establish criminal and civil liability for improper certification or release of keys, provide a market for purchases for government agencies, encourage the development of pilot projects, and negotiate with our trading partners on a common approach to encryption."[26] His comments echoed remarks made by Vice President Gore on July 12th indicating that the administration was willing to consider liberalization of export controls for some encryption products, the establishment of a public-private advisory committee, and possible transfer of jurisdiction for encryption policy from the Department of State to the Department of Commerce. Reinsch cautioned that the administration would prefer to do this through executive action and not through

[25] Hearing of the Science, Technology and Space Subcommittee of the Senate Commerce, Science and Transportation Committee, *Online Security Issues*, chaired by Senator Conrad Burns (R-MT) June 26 and *Encryption* Legislation, chaired by Senator Larry Pressler (R-SD) July 25, 1996. Available through Federal News Service at: http://web.lexis-nexis.com.

[26] Statement of William Reinsch, the Undersecretary for Export Administration in the Department of Commerce, before the Science, Technology and Space Subcommittee of the Senate Commerce, Science and Transportation Committee, July 25, 2001. Available through Federal News Service at: http://web.lexis-nexis.com.

legislation such as S.1726. William Crowell, deputy director of the NSA, also supported a key management infrastructure as the best way of assuring consumer rights and the security of electronic commercial transactions, and emphasized that "only industry can build a robust and scalable key management infrastructure."[27]

Generally, the senators on the Committee appeared more comfortable with a key management system that was implemented without government involvement but many senators – including Senators Hollings (D-SC), Pressler (R-SD), Burns (R-MT), Wyden (D-OR) and Kerry (D-MA) – were concerned with what was referred to as the "genie out of the bottle" question about whether encryption products were already internationally available to countries that might not wish to join key management schemes. Senator Kerry asked whether "if the genie is not out of the bottle today, there is an inevitability to its near-term emergence in such a way that, by restraining ourselves, we are merely disadvantaging ourselves in the marketplace and fighting a phantom that we ultimately can't control."[28] FBI Director Freeh conceded that one of the goals was to "buy some time" and give the U.S. hardware and software industry an opportunity to develop a viable and competitive key escrow system.

On September 25, 1996 the House Judiciary Committee held hearings on encryption controls, specifically on H.R. 3011, the Security and Freedom through Encryption (SAFE) Act introduced by Robert Goodlatte (R-VA) and co-sponsored by a bipartisan group of 45 representatives. The tone and content of this hearing was identical to those of the Senate Commerce Subcommittee hearings with members of Congress voicing strong reservations about a key escrow system that required users to register keys with a trusted third party and about export restrictions on 56-bit encryption that was available on the global market. Although the administration was not yet prepared to announce its new policy, Jamie Gorelick, the Deputy Attorney General, summarized the administration's position as follows: "We would not support the unilateral dropping of our export barriers with no system for the development of a key management system. We believe that there needs to be an internationally adopted key recovery system and that we need to encourage industry to build products consistent with such a system. We would not promote the prohibition of the use of unescrowed encryption domestically."[29] Industry and government witnesses both spoke of the OECD meetings that were occurring at the same time as the hearings and were aware of the need for a global consensus on the issue. The arguments were that, in effect, domestic policies could be circumvented by the policies of another country, restrictive policies in one country were rendered meaningless by the ready availability of encryption on the Internet, and

---

[27] Statement of William P. Crowell, Deputy Director of the National Security Agency, before the Science, Technology and Space Subcommittee of the Senate Commerce, Science and Transportation Committee, July 25, 2001. Available through Federal News Service at: http://web.lexis-nexis.com.

[28] Statement of Senator John Kerry (D-MA) before the Science, Technology and Space Subcommittee of the Senate Commerce, Science and Transportation Committee, July 25, 2001. Available through Federal News Service at: http://web.lexis-nexis.com.

[29] Statement of Jamie Gorelick, Deputy Attorney General of the United States before the House Judiciary Committee, Hearing on Encryption Controls, September 25, 1996 (Federal Document Clearing House, Inc.: FDCH Political Transcripts). Available at: http://web.lexis-nexis.com.

American companies that tried to play by the rules were disadvantaged and forced to use weaker security protections than preferred. By far concerns with industry competitiveness and the workability of a key escrow system dominated the hearing. Despite the Judiciary Committee's jurisdiction, civil liberty interests and law enforcement concerns received scant attention. One shift in emphasis was evident in the testimony of Jamie Gorelick, the Deputy Attorney General, who spoke of the impact on public safety, as opposed to law enforcement, that would be compromised by unbreakable encryption. This seemed to be an attempt to redraw the interests to be balanced in a way that would place more public weight and appeal on the government's interests.[30]

Clipper 3.1.1

In November 1996, President Clinton issued an executive order transferring jurisdiction over personal non-military uses of encryption from the Department of State to the Department of Commerce and permitting companies to export 56-bit encryption if they made "satisfactory commitments" to develop key recovery products. In March 1997, the Commerce Department's Bureau of Export Administration announced easing of restrictions on encryption products used by financial institutions but still required companies to develop law enforcement keys and issue licenses on a case-by-case basis.

During the 105th Congress there were extensive debates on encryption policy. By July 1997, Representative Goodlatte's reintroduced SAFE bill (H.R. 695), which would loosen the export restrictions and allow market forces to determine whether key recovery was adopted, had 255 co-sponsors[31], enough to pass the House. (See Table I for list of supporters and opponents.) In June, FBI Director Freeh told the Senate Judiciary Committee that encryption technology without key escrow would hamper the ability to fight crime and prevent terrorism. SAFE was referred first to the Judiciary Committee and International Relations Committee and then sent to three other committees, National Security, Intelligence and Commerce. The bill passed each committee,[32] but in five different versions with two being complete opposites. In mark-up, the Committee on National Security voted 45-1 to amend the bill and preserve the government's ability to limit exports of the most sophisticated encryption. The amendment was seen as a compromise by its sponsors, Representatives Dellums (D-CA) and Weldon (R-PA), but business leaders saw it as merely a restatement of the administration's current policy.[33] The House Select Committee on Intelligence reversed the intent of the bill and amended it to regulate the production and use of encryption domestically and require use of key

[30] Statement of Jamie Gorelick, Deputy Attorney General of the United States before the House Judiciary Committee, Hearing on Encryption Controls, September 25, 1996 (Federal Document Clearing House, Inc.: FDCH Political Transcripts). Available at: http://web.lexis-nexis.com.

[31] Six of the co-sponsors withdrew their support from July to September.

[32] SAFE was passed by the House Judiciary Committee on May 14, 1997 by voice vote; by the International Relations Committee on July 22, 1997 by voice vote; by the National Security Committee by voice vote on September 9, 1997; by the Committee on Intelligence on September 11, 1997; and, by the Commerce Committee on September 24, 1997 by a vote of 44 to 6.

[33] Hiawatha Bray, "House Committee Backs Clinton on Encryption; US Software Firms Lose Round in Dispute," *The Boston Globe* (Sept. 10, 1997), p. D2.

recovery. This action "spawned outrage among civil liberties groups and computer experts."[34]

After the torturous and inconsistent committee response, the House delayed further consideration until the Rules Committee could attempt to reconcile the multiple and conflicting versions before bringing it to the floor. Representative Gerald Solomon (R-NY), chair of the Rules Committee, opposed Goodlatte's SAFE bill because of its potential harm on national security. Instead, he favored the Intelligence and National Security Committees versions that incorporated key recovery. At the end of the 105th Congress, the SAFE bill was still in the Rules Committee.

On the Senate side, three bills were introduced, each taking a slightly different position but with very similar co-sponsors. Senators Kerrey (D-NE) and McCain (R-AZ) introduced the Secure Public Networks Act (S 909) took a moderate position, relaxing some export restrictions but creating incentives for the public to use key recovery systems. Senator Burns introduced the Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act (S.377) and Senator Leahy introduced the Encrypted Communications Privacy Act of 1997 (S. 376). Hearings were held by the Judiciary Committee in July 1997 on both Senator Leahy's bill and Senator McCain's bill, and by the Committee on Commerce in March 1997 on Senator Burns' bill. In May 1998, a compromise bill was introduced by Senator John Ashcroft (R-MI) with support from Senators Leahy and Burns. The E-Privacy Act, or Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace, provided for: a voluntary key escrow system; enhanced protection for escrowed keys; a relaxation of export regulations for products generally available after a one-time technical review by the Commerce Department; and, the establishment of a National Electronic Technology Center to help law enforcement officials learn to break codes.

During the 105th Congress, changes in policy positions for some advocates and divisions within some coalitions became apparent. A major change was in the position of Dorothy Denning who had been a vocal supporter for the Clipper Chip. A study that she conducted with William Baugh, a vice president at the Science Applications International Corporation, revealed that there were at least 500 criminal cases around the world that involved encryption. Based on this Denning questioned whether legislation would be effective: "I still don't know what the right policy move is on all this."[35] A second change was that business and privacy advocates reached a difference of opinion on Goodlatte's revised SAFE, which business supported but which privacy advocates questioned because of its criminal provisions. There was also some dissension in law enforcement community. This was evident at the March hearings before the Senate Judiciary Committee Subcommittee on Constitution, Federalism and Property Rights, the Executive Director of the Law Enforcement Alliance of America testified that encryption is a tool in preventing crimes. He made two important points: files that are not secure,

[34] Hiawatha Bray, "House Bill Toughens Limits on Encryption," *The Boston Globe* (Sept. 13, 1997), p. F1.
[35] Elizabeth Corcoran, "Encryption: Who Will Hold the Key? Two bills Reflect the Split Over Restrictions" *The Washington Post* (August 4, 1997), p. F15.

can be stolen and misused; and more than 500 encryption products are available on the global market.[36]

Some people in the Administration also appeared to be rethinking their policy positions. In April 1998, Commerce Secretary Daley acknowledged that the administration's attempts to regulate encryption technology had failed.[37] Vice President Gore was also seeking more cooperation between government and industry, preferring to find common ground, without legislation. The Vice President seemed aware of a contradiction between the administration's support for e-commerce and market forces and its support for regulation of encryption technology, especially given the importance of encryption to the success of e-commerce. In order to discuss these issues there was a closed-door meeting in June 1998 between Bill Gates, Microsoft's chairman, and Attorney General Reno and FBI Director Freeh.[38]

In July 1998, the Clinton administration announced that it would permit export of strong encryption without key recovery for banks and financial institutions in 45 countries that have acceptable money-laundering laws. Companies that made software for financial institutions welcomed change but other industry and privacy advocates said policy shift was insignificant. A spokeswoman for ACP said "We don't support this piecemeal approach. We support the lifting of all export restrictions."[39]

By the beginning of the 106th Congress these changes in the policy community were similarly seen in Congress. In April 1999, Senator John McCain (R-AZ) switched his position on encryption legislation and announced that he would join Senators Leahy (D-VT), Burns (R-MT) and Wyden (D-OR) in support of a bill that would relax export prohibitions. McCain – testing waters for a presidential bid.[40] In June 1999 Senator John Kerry (D-MA) also switched position – "restraining our businesses against a sort of phantom menace." Two reports, one by EPIC and one by researchers at GWU, revealed that US was only country attempting to curtail encryption and that high-quality encryption was widely available.[41]

But the Justice Department had not conceded the issue. In fact, in August 1999 it drafted legislation which would permit law enforcement investigators to enter with judicial permission suspects' homes or offices to search for passwords or encryption programs before getting wiretaps or conducting more thorough searches.[42]

---

[36] Ibid.
[37] Alan J. Hoffman and Eric H. Vance, "Sides Debate Future of Encryption: Easy Answers Hard to Find; Privacy Advocates, Law Enforcement at Odds," *New York Law Journal* (July 13, 1998), p. S7.
[38] Jeri Clausing, "Critics Contend U.S. Policy on the Internet Has 2 Big Flaws," *The New York Times* (June 15, 1998), p. D1.
[39] Jeri Clausing, "International Business; White House Yields a Bit on Encryption," *the New York Times* (July 8, 1998), p. D1.
[40] Jeri Clausing, "International Business; Senator Eases Opposition to Encryption Software Exports," *The New York Times* (April 2, 1999), p. C3.
[41] John Schwartz, "Cybertalk; The Key to Unfettered Encryption; Foreign Products May Thwart U.S. Attempts to curb software Exports," *The Washington Post* (June 14, 1999), p. F22.
[42] Steven Lee Myers, "Justice Department Proposing Bill to Foil Computer Encryption," *The New York Times* (August 20, 1999), p. A17.

Exit Clipper

The policy changes that industry and privacy groups had advocated were realized on September 16, 1999 when the White House announced the elimination of its export controls on encryption after one-time review and with a few exceptions to foreign governments, military, and organizations in terrorist countries. In both houses of Congress there was sufficient support for legislation that would have achieved the same result. The House was scheduled to vote later in September on the SAFE bill that had 258 co-sponsors but agreed to stop consideration until the Administration drafted final regulation. Representative Goodlatte said "this is a tremendous victory."[43]

In November 1999 the Clinton administration circulated its draft relaxed encryption regulations but industry and privacy groups said the proposal fell short of what indicated two months ago. They criticized the complicated and ambiguous restrictions regarding sales to governments. Ed Gillespie of the ACP said "Two months ago we were looking at a clean lifting of export restrictions. Now we are looking at a complicated mass of regulations."[44] On January 14, 2000 the Department of Commerce's Bureau of Export Administration (BXA) released revised regulations, conceding to criticisms of industry and reflecting a retreat by NSA and FBI. The new regulations provided for a one time technical review to sell any encryption program and allowed export of "source code" without licenses. In general industry and privacy groups were cautiously positive, noting that the regulations were still complicated and would require legal assistance for many companies and individuals.[45]

Enter Carnivore

During April 2000, Robert Corn-Revere, testifying on behalf of an Internet service provider (ISP) before the House Judiciary Committee's Subcommittee on the Constitution brought to the attention of Congress and the public a new system that the FBI was using to analyze Internet traffic and identify messages. The FBI aptly, but as it later realized unfortunately, referred to this system as Carnivore because of its ability to find the "meat."[46] Carnivore was basically a "packet sniffer" system installed at an ISP to monitor the traffic and select messages that it was programmed to recognize as containing information relevant to an investigation. Although its "black box" characteristics made it immediately suspect, the FBI maintained that this was merely an effort to keep pace with changes in technology and did not represent a change in capabilities or authority.[47] Privacy and civil liberties groups, ISPs, members of Congress

[43] Jeri Clausing, "In a Reversal, White House will End Data-Encryption Export Curbs," *The New York Times* (Sept. 17, 1999), p. C1.
[44] Jeri Clausing, "Concerns Raised Over Encryption Report," *The New York Times* (Nov. 24, 1999), p. C5.
[45] David Sanger and Jeri Clausing, "U.S. Removes More Limits on encryption," *The New York Times* (Jan. 13, 2000), p. C1.
[46] The name provided fodder for press headlines and soundbites: Carnivore would "devour" civil liberties, take a "bite" out of privacy, and had a voracious "appetite."
[47] John Schwartz, "FBI's Internet Wiretaps Raise Privacy Concerns; New System Tracks Suspects Online," *The Washington Post* (July 12, 2000), p. A1.

traditionally supportive of civil liberties, and House Majority Leader Richard Armey (R-TX) were critical of Carnivore and questioned how it met the legal requirements for a wiretap.

By July 2000 the House Judiciary Committee's Subcommittee on the Constitution had scheduled hearings and FBI officials were called to explain how the system worked and how it met traditional Fourth Amendment requirements. Members of Congress expressed concern about the Orwellian Big Brother potential of Carnivore, of the need for law to keep up with technology and to preserve constitutional rights in cyberspace, and of the necessity to control the appetite of Carnivore.[48] One reporter described this as a "bipartisan firestorm of criticism."[49] Witnesses from the FBI argued that it obtained a court order before using the system and that Carnivore was not used for broad searches or surveillance but was a surgical tool with a filtering mask. In addition to technical questions about how the system worked, which were in part addressed by the FBI's web posting of a description of the system, there were two key issues at this hearing and at a subsequent one held by the Senate Judiciary Committee.

The first issue involved the question of whether the Carnivore's capturing of the addressing information on e-mail traffic was analogous to a pen register's collection of calling information. Under Title III and ECPA, a lower level of judicial scrutiny was required for a pen register than for a wiretap.[50] The FBI treated Carnivore as a pen register while many witnesses argued that "T0 and FROM" information in an e-mail was actually content and that a full Title III court order should be required. The law professors and public interest groups, including the ACLU and CDT, that testified at both hearings reasoned that Carnivore was more invasive than a pen register and should require the full Title III court order.

The second issue involved questions about whether the FBI had overstepped its legitimate authority in creating Carnivore and how Congress could effectively oversee operation of the system. The following exchange between Representative Jerrold Nadler (D-NY) and Kevin DiGregory, Deputy Associate Attorney General, is illustrative of the tone and concern.[51]

---

[48] Opening statements of Representatives Canady, Melvin Watt (D-NC), John Conyers (D-MI), Asa Hutchinson (R-AR), and Spencer Bachus (R-AL) at the *Hearings on Fourth Amendment Issues Raised by the FBI's Carnivore Program*, Subcommittee on the Constitution of the House Committee on the Judiciary, July 24, 2000. Available through Lexis-Nexis' Congressional Universe, Federal News Service at: http://web.lexis-nexis.com

[49] Jaqueline Newmyer, "FBI's 'Carnivore' E-Mail Tool Chewed up by Lawmakers," *Los Angeles Times* (July 25, 2000), p. A5.

[50] Pen registers, or trap-and-trace authorizations, required a showing of relevance and certification of relevance by a law enforcement authority. There is no probable cause requirement. There is no requirement to notify the target that the surveillance took place.

[51] *Hearings on Fourth Amendment Issues Raised by the FBI's Carnivore Program*, Subcommittee on the Constitution of the House Committee on the Judiciary, July 24, 2000. Available through Lexis-Nexis' Congressional Universe, Federal News Service at: http://web.lexis-nexis.com

> Rep Nadler: You installed – you started using the Carnivore system about two years ago, and on one ever bothered telling Congress about it; we just found out about it because Earthlink complained about it?
>
> Mr. DiGregory: Well, no one ever bothered telling Congress, in the sense of all of Congress. There certainly have been members and staff briefed on it over the last year.

A similar exchange occurred between Senator Hatch and Dr. Donald Kerr, Director of the FBI Lab Division:[52]

> Sen. Hatch: What authority do you have to do this and to have used it in 25 cases? Has Congress given you any authority?
>
> Dr. Kerr: Well, in fact, Congress appropriated the money pursuant to our budget request within which there is a specific line related to electronic surveillance and particularly the development of tools for access to data networks, the Internet, and the like.

In both the House and the Senate, there was reluctance to "trust" the FBI to "do the right thing" and a recognition of the need to provide for some outside oversight. Although the FBI had agreed to an independent review of the Carnivore system, members were concerned about restrictions that the FBI had placed on the review and the FBI's decision not to release the source code. In response to the FBI's reluctance to reveal information, EPIC filed a Freedom of Information Act (FOIA) request. In August, a US Appeals Court decision ruled that a court-ordered wiretap was required to access digital packets that travel through the cell phone network ; by implication a similar wiretap would be required for Carnivore which accesses packets carried over the Internet.[53]

Although the FBI had agreed to an independent review, Attorney General Reno, in response to concerns of Carnivore's critics and because the FBI was moving too slowly, decided that the Justice Department would share responsibility for selecting reviewers and overseeing the review.[54] The Justice Department reported that it would contact a number of universities, including MIT, Purdue and UC San Diego. Reportedly several universities decline to conduct the review because the government had imposed too many restrictions.[55] On September 26, 2000 the Justice Department announced that the IIT Research Institute at the Illinois Institute of Technology would conduct the review and report by December. Its draft report, issued in mid-November, concluded that Carnivore was a valuable law enforcement tool but that it needed several modifications to better ensure that people's privacy was protected and that searches were limited.[56] A

---

[52] *Hearings on Digital Privacy and the FBI's Carnivore Internet Surveillance Program,* Senate Judiciary Committee, Sept. 6, 2000. Available through Lexis-Nexis' Congressional Universe, Federal News Service at: http://web.lexis-nexis.com

[53] Eric Rosenberg, "Appeals Court Limits Cell Phone Tracking; Decision also Sets Stage for Restriction of Carnivore," *The San Diego Union-Tribune* (August 16, 2000).

[54] David A. Vise, "Quicker Review Vowed for Net Wiretap System," *The Washington Post* (August 4, 2000), p. A27.

[55] Ariana Eunjung Cha, "Carnivore Debate Centers on FBI Trustworthiness," *The Washington Post* (Sept. 7, 2000), p E3.

[56] David A. Vise and Dan Eggen, "FBI Tool Needs Honing; Panel Says 'Carnivore' Software Can Be Altered to Protect Rights," *Washington Post* (nov. 22, 2000), p. A2.

group of computer security experts then challenged that report because of its limited analysis.[57]

With the change of administration came the FBI's change, in February 2001, of the name of Carnivore to DCS-1000 but the name change did not catch on with the press or political community. In April Attorney General Ashcroft met with FBI Director Freeh for a briefing on Carnivore,[58] and soon after met with privacy advocates.[59] In June, Representative Dick Armey (R-TX), a vocal critic of Carnivore, wrote Attorney General Ashcroft asking him to reconsider the use of Carnivore. And, on July 23rd the House of Representatives passed an amendment to the Department of Justice's appropriations bill requiring the Justice Department to give detailed reports to Congress on the uses of Carnivore including who at the Justice Department reviews the requests and the criteria used for approving requests.[60]

Discussion

In general the dynamics of the "separate institutions sharing power" that occurred in the policy deliberations regarding the Clipper Chip and Carnivore are familiar to any student of American politics. The "big ideas" of American politics, most particularly privacy, the First and Fourth Amendments and trust in government institutions, were critical in structuring policy arguments. Interests in global competitiveness, effective law enforcement investigations, and secure communications provided ground for coalition formation and development of pragmatic solutions. And all three branches of government provided access points and forums for policy formation. Several general themes emerge from the Clipper and Carnivore debate and will be discussed below.

First, however, it may be instructive generally to compare the deliberations regarding the two issues. As the policy process unfolded it became clear that Clipper was primarily an issue of technological competitiveness. Business interests and concerns dominated congressional hearings and seemed to motivate changes in administration policy. Without the business support, it would seem that privacy would not have had much traction in defeating the Clipper Chip proposal. Without the support of privacy advocates and civil liberties groups, business would still have had arguments to which the political branches would have listened. Carnivore, on the other hand, elicited a politics and a policy debate that are much more typical of a traditional fourth Amendment issues. The idea of and support for privacy in this debate find a natural ally not in business interests but in the idea of accountability and trust. These ideas resonate loudly on the

[57] John Schwartz, "Computer Security Experts Question Internet Wiretaps," *The New York Times* (Dec. 5, 2000), p. A16.
[58] Eric Lichtblau, "FBI's E-Mail Surveillance Getting Boost; Justice Officials Likely to Call for Continuing Carnivore with Privacy Protections Added," *Los Angeles Times* (April 19, 2001), p. A14.
[59] Jon Sawyer, "FBI's Troubles Could Imperil Its System of E-Mail Surveillance; 'Carnivore' Software Spurs Concerns About Privacy, Agency's power, Critics Say,' *St. Louis Post-Dispatch* (June 3, 2001), p. A1.
[60] H.R. 2215, amendment offered by Bob Barr (R-GA) and passed by voice vote on July 23, 2001.

Hill and in the traditional media. In this case, the issue was helped by the image of Carnivore as a devouring, out-of-control beast.

With these differences in mind, there are still several general themes that merit discussion.

Coalitions Not Tightly Forged, Creatures of Circumstance Not of Conviction

In the debate over encryption policy, the coalition between business and privacy advocates does not represent a completely united front. Industry is willing to make some concessions in order to capture new markets, while privacy advocates are not willing to compromise. Privacy advocates – ACLU, EFF, and EPIC – argued against a key recovery system on First, Fourth and Fifth amendment grounds – banning expression, opening the possibility of secret searches, and forcing people to incriminate themselves – while business saw this primarily as a question of competitiveness. The Alliance of Computer Privacy (ACP) supported Goodlatte's version of SAFE, while the privacy advocate groups questioned the criminal provisions of SAFE. Although several public interest groups, including the ACLU, EFF and EPIC, issued a joint statement supporting ACP and welcoming public debate, none officially joined the coalition. By August 1998, it appeared that the ACP had been successful in achieving a compromise that benefited industry interests. ACP lobbyists conducted briefings with 230 House offices and 30 Senate offices; its representatives held closed negotiations on a possible encryption compromise with officials from the White House, Commerce, Justice, Treasury and Defense.[61] One reporter noted "the effort may someday be cited as a textbook case of how an interest group can use the traditional levers of Washington power ---money, lobbying, public opinion and political connections --- to make the system work for it."[62]

There was far less industry interest and activity in the Carnivore debate. The large ISPs had been quietly cooperating with court orders and did not need the Carnivore system to give the FBI the information it sought. Carnivore was primarily developed for the smaller ISPs who had neither the resources nor the political connections to lobby aggressively. Additionally, it was not in the business interest of either large or small ISPs to have too much public discussion of the surveillance that was possible.

Arena of Expertise not Public Opinion

In an April 1994 article, a *Washington Post* reporter wrote "on purely pragmatic terms, the Clipper initiative seems to have been put together by people who behave as if

[61] These talks were co-chaired by Bruce McConnell of OMB and a lawyer from Arnold and Porter. The government representatives at the talks were assembled by OMB and the National Security Council, which freed them from the reporting requirements for open meetings. Andrew Mollison, "Coalition near compromise on encryption laws; By creating lobbying army, group on cusp of deal with security agencies to allow export of codes," *The Atlanta Journal and Constitution* (August 1, 1998), p. 8A.

[62] Andrew Mollison, "Coalition near compromise on encryption laws; By creating lobbying army, group on cusp of deal with security agencies to allow export of codes," *The Atlanta Journal and Constitution* (August 1, 1998), p. 8A.

they have no understanding of privacy, technology or markets."[63] Both the Clipper and Carnivore initiatives were ones where getting the technical detail correct was perceived as critical to their effectiveness. And in both cases, there was reluctance on the part of the Administration to reveal those details. A good part of the policy formulation for both issues involved rather technical discussions of communications systems, cryptography and global markets. As was demonstrated above, there were several points where the reports or opinions of experts were critical: the Computers, Freedom and Privacy meeting in 1994, the National Research Council Report in 1996, the Ad Hoc Group of Cryptographers and Computer Scientist Reports in 1997 and 1998, the Electronic Privacy Information Center's report in 1999, and the George Washington University Cyberspace Policy Center's report in 1999, and the Illinois Institute of Technology Research Institute review in 2000.

Neither of these issues generated a great deal of public interest or public opinion. The encryption debate was not one that was easily understood by the public and although the ACP did try to broaden interests in the debate it was still fundamentally a technical debate. The debate about Carnivore was a more easily understood issue and one that tapped the public concern about the intrusiveness of government but also public concern about online criminal activity.

Congress as Public Forum, Overseer and Consensus Builder more than Legislator

In the debate over encryption, Congress did not lack statutory proposals that would have eased encryption restrictions and preserved the right of individuals and organizations to domestically use the strongest encryption possible. It also did not lack bipartisan support and active policy entrepreneurs. But when it sensed that the administration would make the changes by issuing regulations, it stepped back. Although the debate over Carnivore has not yet closed, the obvious policy course for Congress is to classify all Internet communications as content and require a full Title III wiretap.[64] This is not a course that Congress has yet taken. In both instances, Congress did not legislate.

It cannot be said, however, that Congress did not play an important role in formulating and even adopting public policy. In both areas, Congress was immediately responsive in scheduling hearings and requiring executive officials to publicly account for their initiatives. In both cases, these hearings provided an opportunity for those on both sides of the issue to hear each other's arguments and, in some cases, to respond to others on the witness panels. And in both cases, the congressional deliberations were instrumental in moving the administration to change policy in ways that did not reflect their most preferred position as seen in the 1999 relaxation of the encryption regulations. Congress may also have been effective in getting the administration to see the larger picture. For example, one analyst noted that "in advancing legislation like SAFE,

[63] Michael Schrage, "Cole Blues: Why the Clipper Chip Plan is Having Unintended Effects," *The Washington Post* (April 15, 1994), p.B3.
[64] Johnny Gilman, "Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications," 9 *CommLaw Conspectus* (2001), pp. 111-129.

Congress pushed the Clinton administration to accept the emergence of a global interconnection that the U.S. cannot exclusively control."[65]

But at the same time, this type of congressional policymaking moves slowly and somewhat indirectly. Congress pushes, the administration signals it will make a change, but then backtracks and Congress pushes again. This scenario benefits those who do not want to change. In this case, this dance worked to the advantage of the government, not industry or privacy advocates. As Michael Froomkin, a professor at the University of Miami School of Law and an expert in cyberspace legal issues, similarly reasoned from the government's perspective "every week where you have a world without mass market crypto, you're ahead…It's a brilliant bureaucratic success story."[66]

Deference to Law Enforcement and National Security Moderated by Global Economic Security

Generally in American politics concerns about law enforcement and national security are treated with utmost seriousness. In the case of the Clipper Chip in particular, this definition of the issue was immediately challenged. The concerns of business competed and redefined the issue to one of global economics. In hearing after hearing, witnesses testified that the "genie was out of the bottle" and that restrictions on encryption technologies would not only be ineffective but were significantly hampering American business. As Melinda Brown of Lotus, representing the Business Software Alliance, testified: "We looked to use solutions that we can implement globally. There are remedies that are apparently available to us through getting waivers for overseas branch offices. We attempted to go down this road…and concluded that the time and effort and the paperwork problems that we had to deal with led us to back off and to use less secure means of communicating with our overseas firms."[67]

There was also a real question about whether the U.S. could or should act unilaterally, In 1997, when the Clinton administration seemed to be loosing ground in Congress with interest gaining for the McCain/Kerrey Secure Public Networks Act of 1997, Clinton sent David Aaron to lobby the OECD for the global adoption of a Clipper Chip type system.[68] Instead, the OECD adopted cryptograpshy guidelines that did not advocate key escrow and shortly thereafter the European Union published a draft paper arguing that market forces and self-regulation should decide encryption policy. In 1998, the Wassenaar Arrangement group, an agreement between 33 industrial countries to restrict exportation of dual-use technologies, rejected key escrow.[69]

---

[65] Tricia E. Black, "Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy," 53 *Federal Communications Law Journal* (March 2001, pp. 289-314), p. 304.
[66] Alan Cohen, "Sides Talk Compromise, but Encryption Policy Lags; Deadlock May be Harder to Break Than Codes Themselves," *New York Law Journal* (April 13, 1998), p. S3.
[67] Statement of Melinda Brown, Vice-President and General Counsel, Lotus Development Corporation before the House Judiciary Committee, Hearing on Encryption Controls, September 25, 1996 (Federal Document Clearing House, Inc.: FDCH Political Transcripts). Available at: http://web.lexis-nexis.com
[68] Lisa S. Dean, "U.S. Encryption Policy Difficult to Encode," *The Seattle Times* (April 21, 1998), p. B5.
[69] Tricia E. Black, "Taking Account of the World as It Will Be: The Shifting Course of U.S. Encryption Policy," 53 *Federal Communications Law Journal* (March 2001, pp. 289-314), p. 302.

Use of Internet to Inform and to Mobilize

For some online policy issues, such as online privacy and online pornography, interest groups have effectively used the Internet to mobilize grassroots interest and support. On these issues, there seems to be less broad mobilization but there is definitely mobilization of computer and cryptography experts and legal specialists. This is not to say that there have not been attempts at mobilizing the public – the CPSR electronic petition in 1994 gathered more than 8,000 signers, but that there has been less online public mobilization than seen in other areas.

Somewhat similarly the Internet has provided an enormous means of public education about policy issues. Again, the online education for the Clipper Chip and Carnivore has been directed more to political elites and policy experts more than to the public as a whole.

Electoral Concerns Play a Role

Policymakers on the Hill and in the Administration were well aware of their constituents' interests on these issues. Both Senator McCain and Vice President Gore were conscious of the position of the high tech community and the importance of that community in fueling economic growth. When the Clinton Administration announced the elimination of export controls in the Fall of 1999, Representative David Dreier (R-CA) attributed the change in part to campaign politics "I think the Administration has finally moved in this instance because of the pressure from we in Congress and Governor George W. Bush, who is getting overwhelming support in Silicon Valley."[70]

Individual members of Congress were also aware of constituent concerns. The interests of constituents, as reflected in the opposition of the American Jewish community, may have influenced Representative Solomon's position. He initially supported the SAFE bill in March 1997 but withdrew his support at the end of April because he decided the original SAFE bill would weaken intelligence gathering capabilities and encourage state-sponsored terrorism.[71] Interestingly encryption policy was of interest to a number of senators and representatives from more rural states where industry was not located. However, for many of them, such as Senator Burns (R-MT), the Internet offered a valuable means of communicating and bringing goods and services to their constituents – but without effective privacy and security protections, they would not take advantage of that potential. And for other members, these issues appealed to their fundamental values about the importance of privacy and limited government. For example, Senator Leahy said "I have the typical Vermonter's view of privacy, that we

[70] Jeri Clausing, "In a Reversal, White House will End Data-Encryption Export Curbs," *The New York Times* (Sept. 17, 1999), p. C1.
[71] Representative Gerald Solomon, "Unlimited Encryption Would Aid Criminals," *Roll Call* (July 13, 1998).

should keep private our confidential affairs from either private sector snoops or unreasonable searches and seizures."[72]

Courts Provide Additional Oversight and Forum

While Congress and the executive branch struggled to formulate encryption policy that would balance privacy, law enforcement/national security, and business interests, the courts were called upon to rule on three individual cases. Both the Departments of State and Commerce refused to grant Philip Karn, a programmer at Qualcomm, a license to export source code for encryption algorithms in electronic form even though the source code was available in print and could be exported in that form. In 1996, a lower court ruled against Karn on narrow grounds and that case is still in the appeals process.[73]

In the second case, David Bernstein, a faculty member at the University of Illinois at Chicago, challenged the export regulations for preventing him form publishing his work and speaking about it at meetings. In three decisions, Judge Patel of the U.S. District Court for the Northern District of California ruled that cryptographic source code is speech protected by the First Amendment, that the encryption licensing scheme is a prior restraint, and that the encryption export regulations were unconstitutional as a prior restraint on protected speech.[74] The Ninth Circuit Court of Appeals agreed that the export regulations constituted a prior restraint on speech but noted that not all software could be considered expressive and hence speech. The Justice Department asked for an *en banc* review.

The third case was brought by Peter Junger, a law professor at Case Western Reserve, who was denied permission to "export" source code by posting his own encryption programs and the source code for PGP and RSA on his website for students in his Computers and the Law course. The lower court ruled against Junger holding that exporting software is not expressive.[75] He appealed this decision and in April 2000 the Sixth Circuit Court of Appeals ruled for Junger holding that source code is an expressive means for exchanging information about computer programming and is protected by the First Amendment.[76]

---

[72] *Hearings on Digital Privacy and the FBI's Carnivore Internet Surveillance Program,* Senate Judiciary Committee, Sept. 6, 2000. Available through Lexis-Nexis' Congressional Universe, Federal News Service at: http://web.lexis-nexis.com

[73] *Karn v. US Department of State*, 925 F. Supp. 1 (D.D.C. 1996) and *Karn v. US Department of State*, 107 F.3d 923 (D.C.Cir, 1997).

[74] *Bernstein v. US Department of State*, 922 F. Supp 1426 (N.D. Cal 1996), 945 F. Supp 1279 (N.D. Cal. 1996), and 974 F. Supp. 1288 (N.D. Cal 1997).

[75] *Junger v. Daley*, F.Supp (N.D.Ohio 1998).

[76] *Junger v. Daley*

The Supreme Court's recent decision in *Kyllo v. United States* restricting the use of thermal-imaging technology because of its undermining of the expectation of privacy may also have implications for Carnivore type surveillance systems.

Conclusion

In closing, the policy debates and decisions about online encryption and wiretapping do not appear to indicate that cyberspace has ushered in a new rearrangement of American politics and policymaking. There appears to be no populist electronic uprising, no abdication of the rule of law, and no revolution in ideas and values. Instead, the traditional institutions and processes of American government are "muddling through" to determine how law and policy can accommodate the technological changes. Interest groups and business are applying their conventional lobbying techniques and coalition building to pressure decisionmakers.

Table I
Partial List of Supporters and Opponents
SAFE (H.R. 695)

Supporters of H.R. 695	Opponents of H.R. 695
U.S. Chamber of Commerce	National Sheriffs' Association
National Association of Manufacturers	International Association of Chiefs of Police
Law Enforcement Alliance of America	District Attorneys Association
Business Software Alliance	Veterans of Foreign Wars
Computer & Communications Industry Assoc.	B'nai B'rith
Information Technology Assoc.	
Netscape	
Microsoft	
Americans for Tax Reform	
Eagle Forum	
National Rifle Association	
ACLU	
Center for Democracy and Technology	
Americans for Computer Privacy	

Source: Rep. Bob Goodlatte, "How should Congress act to protect privacy on the Internet? SAFE Act Protects Personal Privacy," and Rep. Gerald Solomon, "Unlimited Encryption Would Aid Criminals," *Roll Call* (July 13, 1998).

.

Timeline

1993, April	Clinton administration proposes legislation requiring the incorporation of the Clipper Chip into all encryption products. The Clipper Chip was developed by the National Security Agency.
1993, May	Digital Privacy and Security Working Group – formed over a decade, coalition of over 50 organizations, including computer software and hardware firms, telecommunications and energy companies, the ACLU, and EFF-- asked for public dialogue and sent Clinton list of over 100 questions.
1994, February	White House announced adoption of Clipper Chip; Attorney General Reno announced two government agencies will hold escrowed keys. Department of State designated cryptographic systems and software as "munitions" requiring a license for import or export.
1994, May	House Hearing on Communications and Computer Surveillance, Privacy and Security, Committee on Science, Space and Technology Subcommittee on Technology, Environment and Aviation.
1994, October	Communications Assistance for Law Enforcement Act (CALEA, aka the digital telephony law) signed into law. Required telecommunications carriers to ensure that their equipment is wiretap-friendly. Industry support secured after Administration promised to seek $500 million from Congress to fund the program.
1995, September	At NIST conference, Clinton administration announced the commercial Key Escrow initiative, "Clipper II," which relaxed export controls on key lengths up to 64 bits if an encryption key was escrowed with a US government certified agent.
1995, October	FBI sought authority under CALEA to monitor one out of every 100 telephone lines in "high crime areas."
1996, March	Rep. Goodlatte (R-VA) introduced the Security and Freedom through Encryption Act (SAFE) (H.R. 3011) and Senator Leahy (D-VT) introduced Encrypted Communications Privacy Act (S. 1587).
1996, May	National Research Council issued its report *Cryptography's Role in Securing the Information Society* which was somewhat skeptical of key recovery systems and advocates more open discussion of encryption policy.
1996, May	Clinton Administration released its Clipper III proposal which would establish a "public key infrastructure" for encryption, ensure government access to encryption keys through approved key escrow agents, allow export of software programs using 64 bit keys if escrowed and hardware with 80 bit keys, and permit large U.S. to escrow own keys.
1996, October	Daniel Bernstein filed suit against the State Department arguing that the export control laws violate the First Amendment.
1996, October	Clinton administration announcement of plan to ease export controls; response in part to IBM and other industry leaders. Interagency Working Group on Encryption to consult with interested parties.
1996,	Clinton signed an executive order, known as "Clipper 3.1.1," giving

November	Commerce Department the exclusive authority over encryption export regulation and permitting export of 56 bit encryption systems if there were commitments to develop key recovery products. Business Software Alliance, including IBM, were critical
1996, December	Federal District Court judge ruled that the International Traffic in Arms Regulations governing encryption are unconstitutional.
1997, March	OECD guidelines reject key escrow encryption and endorse strong privacy standards.
1997, August	Federal district court judge ruled in *Bernstein v. Department of* State that encryption export regulations violate the First Amendment; government appeals.
1997, November	Civil liberties groups petition the FCC to reconsider and bar FBI's plans for expanded wiretapping capabilities under CALEA.
1998, February	Americans for Computer Privacy, coalition of high tech companies and privacy advocates, formed.
1998, April	NSA issues report, *Threat and Vulnerability Model for Key Recovery*, detailing risks of key recovery systems.
1998, September	Clinton administration announced export of 56 bit encryption products after a one-time government review, allow export relief for some industries, and provide exemptions for "recoverable" products.
1999, February	SAFE (H.R. 850) reintroduced in 106th congress.
1999, June	Justice Department circulated draft Cyberspace Electronic Security Act (CESA) bill which would have allowed federal agents with search warrants to secretly break into homes and offices to obtain decryption keys or passwords and to modify computers so that encrypted files or messages could be read by the government.
1999, September	Justice Department officially proposed redrafted CESA without the secret searches provision but also without requirement of probable cause and notice of a seizure.
1999, September	Clinton administration announced reform of export controls, with final regulations released in January 2000. Permitted export of most encryption products regardless of their strength or the type of technology used.
2000, April	FBI developing a new generation of digital tools, known as Digital Storm, to sift and link data from different sources.
2000, July	FBI releases description of Carnivore, a computer program designed to intercept Internet communications.
2000, July	House Judiciary Committee holds hearings on Fourth Amendment issues raised by FBI's Carnivore program.
2000, August	DC Federal Court of Appeals overturned in part an FCC ruling under CALEA ordering carriers to provide additional call dialing and signaling information but upheld the FCC requirement for the location of wireless phones.
2000, September	Senate Judiciary Committee holds hearings on Carnivore