

Listening in on DC: Soviet Eavesdropping and the Origins of US Privacy Policy

Abstract

The discovery of Soviet eavesdropping on US telecommunications by the Ford Administration in 1974 set off a chain of events that culminated in the creation of the first substantive US government policy on electronic privacy and security. This discovery combined augmented privacy concerns raised in the aftermath of the Watergate scandal and led the Ford administration to formulate federal information privacy policy for the first time. This policy study recognized the vulnerability of government information because of the growing link between computers and telecommunications systems. The Ford's National Security Council took measures to secure the US telecommunications infrastructure from foreign eavesdroppers with a clear understanding of the convergence of computers and telecommunications technologies by ordering the Office of Telecommunications Policy and the National Security Agency to examine the problem and recommend remedies. These policies were interwoven with the intelligence community's concerns over communications security and access to signals intelligence as well as concerns about the US telecommunications market structure. Soviet eavesdropping set in motion the development of modern information privacy policy centered on national security and intelligence priorities and this has been the foundation upon which US privacy policy has been built.

John Laprise is a doctoral candidate in the Media, Technology, and Society program with the School of Communications at Northwestern University. Mr. Laprise has been interested in ICTs and national security issues since receiving his MA in War Studies at King's College-London for his thesis on applying maritime warfare doctrine to the Internet. His dissertation examines the adoption of ICTs by the Nixon, Ford and Carter administrations and their influence on the formation of US ICT policy.

Introduction

In June 1975, the Rockefeller commission released its final report on CIA activities within the United States. The published report focused on the CIA's illegal activities in monitoring and disrupting political groups within the US. In the course of the commission's investigation it collected a large amount of information through interviews, testimony, and documentary records on a broad range of interrelated topics. One topic briefly addressed in the report was the vulnerability of telephone conversations to foreign intelligence services. The report stated:

While making large-scale use of human intelligence sources, the communist countries also appear to have developed electronic collection of intelligence to an extraordinary degree of technology and sophistication for use in the United States and elsewhere throughout the world, and we believe that these countries monitor and record thousands of private telephone conversations. Americans have a right to be uneasy if not seriously disturbed at the real possibility that their personal and business activities which they discuss freely over the telephone could be recorded and analyzed by agents of foreign powers

This raises the real specter that selected American users of telephones are potentially subject to blackmail that can seriously affect their actions, or even lead in some cases to recruitment as espionage agents. (Report to the President by the Commission on CIA Activities within the United States)

These statements diminish the true scope of the problem revealed by the Rockefeller

Commission's work as an earlier draft version includes the following more ominous analysis:

While making large-scale use of human intelligence sources, the communist countries also appear to have developed electronic collection of intelligence to an extraordinary degree of sophistication. Recent defectors report that these countries regularly monitor and record most of the telephone communications in major population centers of the United States. Hundreds of thousands of conversations are thus being intercepted, with particular numbers sorted out by the use of computers. Radio microwave transmissions, which carry most of the communications in the United States, can be and are being monitored and transcribed on a regular basis, night and day. American users of telephones who have anything to hide are therefore potentially subject to blackmail that can seriously affect their actions, or even lead in some cases to recruitment as espionage agents.

These foreign invasions of the privacy and security rights of Americans therefore demand our most serious concern. They do not in any sense justify unlawful activities of the CIA which impinge on the privacy and rights of American citizens. But they do argue strongly for strengthening the counterintelligence activities of the FBI within the United States, and for maintaining, if not increasing, the CIA's capacity for collecting foreign intelligence. (Rockefeller Commission Report: Working Copy)

This disturbing finding did not surprise the Ford Administration which began securing US telecommunications systems immediately after taking office in August 1974 by issuing National Security Decision Memorandum (NSDM) 266 "Improved Security of Telecommunications".

Ford was well versed with information policy, having led then President Nixon's Domestic Council Committee on the Right of Privacy. In this capacity, Ford and his advisors became aware of the technological trends leading to the convergence of computers and

telecommunications networks. During the next three years, President Ford issued three additional NSDMs on the security of US telecommunications. The Ford administration studied, proposed, and implemented a range of privacy measures designed to protect the vast amount of information collected and held by the US government

The actions of the Ford Administration are a watershed in US information policy. During the Nixon administration, the White House adopted computers and discovered that computers were more than specialized engineering calculators; they were information organization and analysis engines. Ford's role as head of the Domestic Council Committee on the Right of Privacy informed his thinking as President following Nixon's resignation. The Ford White House understood the power of interconnection and viewed telecommunications and computers together. When Soviet eavesdropping on telecommunications on US telecommunications was identified, the White House viewed it as a significant threat to US national security because it allowed the USSR access to valuable information government collected by the US government. The Ford Administration developed the first US information and privacy policies in response to the Cold War surveillance threat posed by the Soviet Union. Privacy was a Cold War defense of information.

Prelude: The Domestic Council Committee on the Right of Privacy

The Domestic Council Committee on the Right of Privacy (DCCRP) was formed by then President Nixon in 1974 and chaired by Vice President Ford. Nixon formed this committee based on growing concerns about "Big Brother" style information control and management. In his State of the Union address Nixon described this effort: "Modern information systems, data banks,

credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another---all these have left millions of Americans deeply concerned by the privacy they cherish.” He went on to promise that he would “establish a new set of standards that respect the legitimate need of society, but that also recognize personal privacy as a cardinal principle of American liberty.” (Richard Nixon: Address on the State of the Union Delivered Before a Joint Session of the Congress.)

These brief sentences convey the thinking of Nixon’s assistant for Domestic Affairs Kenneth Cole. In a January 1974 memo, Cole suggests to Nixon that personal information is owned by the individual and that the business of society is conducted smoothly when this privacy is protected. New technology had greatly improved information sharing but had also made information protection more difficult so the government should define and protect privacy in the face of technological change. Cole noted that these concerns notwithstanding, privacy did not provide protection from overriding government responsibilities in areas such as criminal intelligence and national security. (Memo From Ken Cole to President Nixon, 1/24/74)

Cole organized his thinking about privacy into broad categories with associated problems and principles. Cole’s operationalization of privacy resembles that of modern “opt-in” privacy standards that are in force in the European Union.

Table 1: Nixonian Privacy Issues

Functional Category	Problems	Principles
Collection of information	<ol style="list-style-type: none"> 1. Legality and relevance 2. Technology 3. Pervasiveness 	<ol style="list-style-type: none"> 1. Individual right to discover information collection 2. Individual requirements 3. SSNs
Storage of Information	<ol style="list-style-type: none"> 1. Security 2. Facilities 	<ol style="list-style-type: none"> 1. Security for personal data 2. Access and ability to correct personal data 3. Shared vs. dedicated government data systems
Use and dissemination of information	<ol style="list-style-type: none"> 1. Misuse 2. Organizational 	<ol style="list-style-type: none"> 1. Individual knowledge of use 2. Individual ability to stop the use of information 3. Organizational responsibility

The initial meeting of the DCCRP occurred in February 1974. President Nixon and Vice President Ford conveyed Cole's privacy framework to the assembled membership including the secretaries of the Treasury, Defense, Commerce, Labor, Health, Education and Welfare, the Attorney General, and the directors of the Office of Management and Budget, Office of Telecommunications Policy, Office of Consumer Affairs, and The Domestic Council. These entities were chosen because of their use of information. Despite the authority of these individuals, Nixon made clear that privacy policy was a "very political and sensitive area" and policy would be crafted by committee discussion and not by the staff. (Meeting with Domestic Council on Privacy from Geoff Shepard)

The reasons for members' selection to the DCCRP was made clear in the DCCRP's draft action plan of March 1974 which identified three objectives: to organize and staff the DCCRP, to begin short range plans that could be accomplished within four months within the executive branch, and to examine long range plans that would take longer than four months. The action plan outlined goals and projects that reflect Cole's privacy issues as articulated to Nixon earlier. The short term projects included restricting the use of SSNs, and protecting statistical data, IRS taxpayer data, Federal civilian data, Uniformed Military personnel data, and Federal contractor and grantee data. Long term projects included the development of state and local statutes, strengthening the Fair Credit Reporting Act, and implementing a code of fair information practice for the private sector. (Proposed Action Plan for the Domestic Council Committee on the Right of Privacy, 3/13/74)

The DCCRP had modest success within the executive branch as departments began examining their inventory of citizens' information and devised measures to protect it. Ideas such as encrypting information and securing computers for controlling electronic information and access control for paper files were shared among the DCCRP in memos and discussions. The Departments of Labor, Commerce, Justice and the OTP were among the most active departments in this respect. Labor, Commerce and Justice as well as the IRS and FTC collected and retained significant information about citizens. (Annual Report of the Privacy Protection Study Commission, 6/76; Privacy Initial Department and Agency Recommendations) Meanwhile, Commerce and OTP were struggling for control of US executive telecommunications and information policy. The Nixon administration's role in the Watergate scandal eroded government credibility and undercut the efforts of the DCCRP to protect the privacy of citizens. As events culminated with Nixon's resignation, newly sworn in President Ford appointed Vice President Rockefeller to lead the DCCRP. Rockefeller immediately began working on problems of privacy and security.

National Information Policy Report

In September 1976, the DCCRP under Nelson Rockefeller's leadership issued its National Information Policy Report. President Ford had instructed the DCCRP in the previous March to examine information policy issues facing the federal government, report on the progress of existing investigations within the government and make recommendations on how the government should organize itself to make and implement information policy. This order stemmed from work that the DCCRP was already pursuing having convened a Roundtable on Privacy and Information Policy in September 1975 and other meetings examining the expanding sphere of issues interlinked with privacy.(National Information Policy Report, 9/1/76)

The Report recommended that the US pursue a unified and coordinated National Information Policy by establishing an Office of Information Policy (OIP) in the executive office of the President. It also recommended the creation of a Council of Information Policy comprised of senior agency representatives and led by the director of the OIP and an Advisory Committee drawing upon expertise in the private sector to assist the OIP in its duties. The Report made these recommendations having identified “information policy” as an exceedingly broad topic that demanded a wide range of perspectives. (National Information Policy Report, 9/1/76)

Despite the breadth and complexity of “information policy”, the authors made seven parting suggestions for the future work of the proposed OIP:

- Encourage open and equal information access for all
- Protection of personal information and protection of individual rights to safeguard that information
- Encourage systems that create and distribute knowledge
- Appropriately regulate the power available to the government through the use of information systems
- Encourage efficient information systems
- Support private sector competition in information technologies to strengthen innovation
- Make rules that embody stability in spite of technological change to encourage private sector technology adoption

The OIP would not come into being but the model would be influential in the simultaneous debate going on in the NSC over telecommunications security. The proposed OIP was very

similar to the entity suggested by the NSC to make telecommunications security policy in structure, membership, and resources. Similarly, the policy suggestions made by the report resemble many of the NSC's telecommunications security concerns on issues such as encouraging technological innovation, public access, and private sector competition. (National Information Policy Report, 9/1/76)

Telecommunications Security and The Rockefeller Report

Another area in which Vice President Rockefeller encountered privacy and information policy issues was in the intelligence and security related portfolios under his management. As chairman of the Commission on CIA Activities within the United States, he led the investigation to discover how the CIA had operated within the US in a manner contrary to its charter. The commission's original mandate stems from President Ford's order to examine whether the CIA had violated the privacy of US citizens and had participated in the assassination of foreign leaders and the report focused on these questions. But as previously noted, Soviet eavesdropping on the U.S. telecommunications system threatened U.S. national security. The Commission asserted in its final report that the protection individual liberties and rights was of primary concern to the government and any organization infringing these rights must be held accountable. At the same time, the commission acknowledged the necessity of national intelligence regulated by the government and noted that it was essential for public safety. Public safety and personal liberty were mutually supportive and essential qualities of American society. (Rockefeller Commission Report)

The Rockefeller report examined in detail a wide variety of the CIA's surveillance activities that violated individual rights. Surveillance of telegraphy, mail, electronic surveillance and

wiretapping were all activities undertaken by the CIA within the US against US citizens in spite of the CIA's charter which mandated that its activities be conducted outside the US. In the course of their research on surveillance, Rockefeller and the commission acquired an understanding of electronic surveillance and became more aware of the vulnerability of US telecommunications networks. (Rockefeller Commission Report)

Telecommunications Security and DUCK PINS

Prior to Rockefeller's appointment to head the DCCRP, the protection of individual information was superseded by the Cold War threat of Soviet eavesdropping and capture of personal information. Protecting citizens' personal information from the US government and private industry was secondary to protecting such information from foreign governments. Following his inauguration in August 1974, The National Security Council informed President Ford that the nation's telecommunications systems were unsecure and that the Soviet Union was intercepting US telecommunications. Telecommunications security would be a preoccupation for the Ford Administration which issued four NSDMs on the topic during his three years in office.

Table 2: Ford Telecommunications Security Timeline

Date	Event
8/9/74	Gerald Ford takes office
8/15/74	NSDM 266 Improved Security of Telecommunications
5/23/75	NSDM 296 Improved Communication Security
9/1/76	NSDM 338 Further Improvements in Telecommunications Security
1/18/77	NSDM 346 Security of US Telecommunications
1/20/77	Gerald Ford leaves office

President Ford issued National Security Decision Memorandum 266 on August 15 to the Secretary of Defense that "immediate defensive steps be taken" to

combat the potential for Soviet interception of microwave communications in the Washington DC area. The Department of Defense along with the Office of Telecommunications Policy were

placed in charge of this effort which in the short term would move threatened US government communications to wired connections and in the long term look to secure wireless communications or expand wired connectivity. Ford informed the State Department, Office of Management and Budget, and Central Intelligence Agency of this plan. (National Security Decision Memorandum 266)

DUCK PINS was the code name given the US government's short term plan to secure US telecommunications in the Washington DC area. This plan involved transferring sensitive governmental telecommunications to wireline networks. DUCK PINS immediately began to ruffle feathers. In 1974, the FCC was in the process of deregulating the long distance telephony market to allow new companies such as MCI to compete. Relatively inexpensive microwave towers and satellites enabled MCI and other AT&T competitors' to compete and were their primary mode of transmission but NSDM 266 had deemed them vulnerable to Soviet eavesdropping. The incumbent AT&T had a large and secure wireline infrastructure. AT&T was the immediate beneficiary of DUCK PINS as it was the only carrier that could immediately offer the wireline services demanded by NSDM 266. (Memo from Charles Joyce to Gordon Moe, 11/26/74)

This situation was delicate as the General Services Administration (GSA) was in the process of bidding out government telecommunications circuits between Washington DC and New York City. The NSC perceived that AT&T's competitors would submit attractive bids to wrest lucrative government business away from AT&T. Unfortunately, since their service failed to meet the new requirements for secure governmental communications, they would have to be

passed over. The government had to find a publicly acceptable reason for passing over competitive microwave based bids. DUCK PINS had the potential to undercut deregulation through the secret adoption of telecommunications security measures and parameters. (Memo from Charles Joyce to Gordon Moe, 11/26/74)

In the long term, DUCK PINS was similarly problematic to deregulation. DUCK PINS called for all government and private communications to be protected from interception. Previous to deregulation, this would be easy to accomplish through discussions with AT&T. With deregulation, the NSC saw that it would be difficult if not impossible to support deregulation while only contracting with AT&T. Eventually; the US government would be called upon to explain why it only dealt with the incumbent and face the politically unacceptable outcome of publicly revealing the vulnerability of the US telecommunications infrastructure. Alternately, the US government would have to select some of the new telecommunications companies, informing them of the security situation and working with them to implement security.

One solution to this problem that was discussed was to limit the telecommunications lines that needed to be protected. Among those singled out for protection were the growing data systems of the GSA, Social Security, and Veterans Administration which compiled computerized information on the millions of citizens served by these organizations. The NSC recognized that trying to protect Washington DC communications would take time.

The NSC's telecommunications panel worked through these issues throughout the Ford administration and initiated the Executive Secure Voice Network (ESVN) and Protected Radio

Modulation (PRM) to protect microwave transmissions. It also began examining cryptography as a long term solution for data protection. This progress was affirmed in May 1975 by NSDM 296 which acknowledged the ongoing conversion of government microwave links over to cables and enjoined government agencies to continue this process. It also continued to emphasize that the problem of telecommunications security in the US should continue to be kept out of the public eye, in spite of the potential for publicity during the implementation of PRM.(National Security Decision Memorandum 296, page 1)

In 1976, the Telecommunications Panel discussed a point paper examining the government's role in providing cryptographic systems and insuring their integrity and security. Integrity and security were key to protecting US military, diplomatic, economic, and technological interests. Secondly, it would be implemented to protect US citizens their right to privacy. Conceptually, the NSC asserted that the US government had a "unique" capability in cryptography and that it should take the lead role in developing, testing, and distributing cryptographic systems. The NSC also envisioned that a portion of the cryptokey would be kept from the US government through an escrow system to assuage the public's privacy concerns. Finally, the NSC believed that common carriers would be participants in the development and deployment of such systems owing to their expertise in communications networks. The point paper advocates a complete US government monopoly on cryptographic materials and systems. It provides no evidence that cryptographic systems were to be used in an offensive manor and that government participation was due solely to the expertise that resided in such places as the National Security Agency. (Point Paper, 8/28/76)

Cooperation with the common carriers became an ongoing theme of the planning of DUCK PINS. A July 1976 paper making recommendations on the implementation of multichannel radio protection stakes out clear positions that about the interrelationship of government, business, and the public. The paper advocates seeking voluntary cooperation with microwave and satellite carriers noting that imposing a requirement would require public disclosure of the threat of interception and take time to navigate regulatory and judicial issues that would arise. Voluntary cooperation, the paper notes would require the establishment of standards and well-defined procurement practices. It also noted the importance of bringing carriers other than AT&T into the program swiftly to allay competitive concerns that AT&T had an unfair advantage. AT&T had made presentations and been involved in the planning of DUCK PINS because of its technological and infrastructural advantages. (Policy Issues and Associated Legal and Regulatory Factors Involved in Implementing Multichannel Radio Protection, 7/7/76)

The paper next recommended that national security rather than individual privacy should be advanced as the main reason for the protection of communications. The report noted that Vice President Rockefeller had already informed the public about the threat in the Rockefeller Commission report. Unfortunately the public was unimpressed by government's efforts to protect privacy and would be skeptical about the new regulatory and legal mechanisms which would be required. By invoking national security concerns, these hurdles could be bypassed or avoided by keeping out of public view.

The paper also proposed that the carriers be brought into the program through an industrial advisory committee so that they could all be kept abreast of technology, plans, and policies. The

paper further suggested that this advisory committee be formed under the auspices of the executive branch rather than the FCC or an advisory group so that issues can be raised and discussed in a timely fashion. Here again, the paper warned that if all carriers were not together, it was highly likely that uninvited carriers would perceive government favoritism, complain, and make the program public. The authors did not see giving cryptologic technology to the carriers as a problem. While they recommended that the government supply and maintain all cryptographic materials they also felt that the US government could serve in this role without becoming enmeshed in the operations of carriers' facilities by using sufficiently trained and vetted personnel from the carriers.

NSDM 338

NSDM 338 "Further Improvements in Telecommunications Security" issued in September 1976 remains classified. (National Security Decision Memorandums (NSDM) [Ford Administration, 1974-77]) However, the Report of the Special Task Group on Telecommunications Organization issued in December 1976 sheds light on the thinking of the Ford administration following the development of DUCK PINS and the content of NSDM 338. NSDM 338 directed the creation of the Special Task Group whose members were drawn from the NSC, OMB, OTP, the Domestic Council and the White House Counsel's Office to examine the implications and ramifications of protecting private sector microwave communications. Specifically, the Task Group was asked to examine the idea of creating a new government entity or reconfiguring an existing entity to manage the telecommunications security program. NSDM 338 noted that the entity should be evaluated on a range of criteria including its ability to examine telecommunications policy issues, program management, authority and ability to act within the government, funding,

manpower, and access to the intelligence community.(Report of the Special Task Group on Telecommunication Organization, 12/1/76)

Noting that the government had already taken steps to protect critical governmental information, the report goes on to say that government has an important role in preserving national communications security as it the repository for cryptographic expertise and provides the standards and policies that enable the continuing function of a nationally integrated telephone system. The report emphasizes the need for the government to create a “favorable climate for public acceptance of communications security so that it is perceived as a means to increased privacy and not as a threat.”

The report suggests two ways for the government to protect communications which echo the thoughts and concerns of Joyce and Moe in 1975. The government could mandate a program but this would require significant government intervention into the market and would likely include difficult and “politically sensitive” decisions about what parts of the private sector to protect. Alternately the government could encourage the private sector to take on this project by providing key parts of research and technology, establishing standards and policy, and educating the industry regarding the importance of secure communications. Both options involved significant financial, regulatory, and legal challenges that required the cooperation of multiple government agencies Moreover, the cost and effectiveness of the new technologies to protect microwave transmissions were unknown and these initiatives could seriously impact the move towards the deregulation of the common carrier market. All of these issues were to be addressed in a report authored by the OTP.

To implement these plans, the report saw the need for a government entity that could address all of the varied and complex issues. The report noted that to date, these matters had been handled in an ad hoc way by the NSC with assistance from the NSA, DOD and OTP with the Department of Justice contributing to threat assessments. While the NSA would have been a logical choice based upon their signals intelligence expertise, the Task Group deemed the political sensitivity of assigning telecommunications to an intelligence organization unworkable. The Task Group proposed six possible entities: a cabinet committee reporting to the President and supported by a private sector advisory board; a joint government committee in the Office of the Vice President supported by a private sector advisory board; continuation of NSC oversight; assignment to a single cabinet office; formation of a new organization in the Executive branch and reporting to the President; and designation of an existing organization in the Executive branch and reporting to the President. All of these possibilities included pros and cons relating to the criteria laid out in NSDM 338.

The Report concluded with a series of observation and criteria as it did not want to make recommendations to a new administration.

- The Task Group noted that the first three organizational options were better suited for a more passive governmental role while the latter three would support more aggressive government intervention.
- Cooperation with industry was preferable to federal mandates.
- Competition should continue to be encouraged and security programs should be designed with this in mind.

- The organization must be consultative in nature, but have authority to implement decisions.
- The organization must have expert staff to provide support to the decision making process.
- The organization should not be perceived as a military or intelligence arm of the government by the public so that it will receive public support but at the same time needs direct participation and cooperation with the NSA.
- The organization needed input from the private sector, as stakeholders.

With these criteria in mind, the Task Group favored the creation of a cabinet committee or a government committee in the Office of the Vice President. The Task Group felt that the NSC did not have the proper staff for implementation. Designation of a cabinet portfolio or creation of a new executive office would be advisable only if the government proceeded to issue mandates. Finally, they believed that designation of an existing executive branch agency was inadvisable as their fortunes and influence waxed and waned from administration to administration. The Task Group's finding mirrored those of the Privacy Commission's call for an Office of Information Policy and this is unsurprising given that the authors of these reports had significant overlap including the Vice President and members of both the Domestic Council and the NSC. (Report of the Special Task Group on Telecommunication Organization, 12/1/76)

Ford's Final Decisions

In January 1977, Ford received a memorandum from National Security Advisor Brent Scowcroft and Jim Cannon, Assistant for Domestic Affairs and Director of the Domestic Council on the status of DUCK PINS and associated programs. Ford faced the decision of whether to expand

protection to all domestic communications or limit it to sensitive government communications only. Guiding his thoughts were two reports; a damage assessment to US interests prepared by the intelligence community and technical assessment of US capabilities to protect telecommunications. (Memo from Brent Scowcroft and Jim Cannon to the President, 1/6/77) The threat report concluded that US microwave telecommunications were at continuing risk of interception. The technical assessment asserted that there were no insurmountable technical challenges to deployment, while noting that an “evolutionary approach” utilizing a range of technologies would be necessary to adapt and protect the expanding range of telecommunications.

The memo then focused on two key policy questions; whether to protect the private sector and whether to tell the public about the problem. In arguing to protect the private sector, Scowcroft and Cannon stressed that making a decision would emphasize to the incoming Carter administration the importance of the issues at hand. There was also direct evidence that US national interests were being significantly damaged by Soviet eavesdropping. Finally, if the government did not act and US vulnerabilities became known to the public, private sector carriers would implement security in a piecemeal manner that might not be effective. Scowcroft and Cannon also cite two drawbacks of protecting private sector communications. First, such protection might compromise existing US signal intelligence capabilities being used against the Soviets by identifying and addressing the problem. Second, many of the new common carriers were struggling financially and new equipment might be a significant competitive disadvantage.

With respect to the question of informing the public, Scowcroft and Cannon identify a number of advantages. Private organizations, once warned will take independent measures to protect information. Public disclosure would put the Administration's efforts in the "right perspective." At the time there were a variety of investigations dealing with government invasions of privacy and the public was concerned about the infringement of their civil rights by government, military and intelligence organizations. Identifying the Soviet threat would explain government actions. Public explanation would also assist in the research, development and deployment of security technologies as the private sector would be more disposed to cooperate. Finally, public disclosure would force the incoming Carter Administration to continue to address the issue. The unredacted disadvantages of public disclosure include generating anti-Soviet sentiment and creating a panic leading to a headlong rush for more security than current technology is able to provide. Scowcroft and Cannon go on to discuss implementation and organizational options for the Task Group report.

Other presidential advisors weighed in on this decision. Ed Schmultz and Philip Buchen of the White House Counsel's office emphasize the importance of carefully explaining the program to the public and Congress so as to allay any fears of the military and intelligence communities' access to the public communications network (Memo from Jim Connor to the President, 1/12/77). In the end, President Ford agrees to implement private sector protection but chooses not to make the telecommunications situation public. He further agrees to create a joint committee to be created by the NSC and the Domestic Council and chaired by Vice President Rockefeller, who had contributed to the discussion and voiced concerns about US telecommunications security.

NSDM 346

Four days after President Ford signed the memo ordering the protection of private sector telecommunications and concealing the problem from the public, he issued NSDM 346 “Security of US Telecommunications” which is prefaced by an acknowledgement that microwave radio is unsecure and easy to intercept. (National Security Decision Memorandum 346, page 1) It goes on to relate that Washington DC government microwave communications have been moved to cables and that government communications in New York and San Francisco were in the process of being moved to cable. Communications links between the government and sensitive government contractors were also being protected. Microwave communications protection equipment was being developed by the DOD and would be tested in Washington DC within the year and the OTP had developed for a deployment plan to cover these three key cities and later the rest of the nation. NSDM 346 then announced the formation of the joint committee chaired by the Vice President and tasked it with deciding whether to encourage private sector cooperation by requiring secure communications in government communications and thereby create standards and work with the common carriers; or to mandate a protection scheme throughout the national network and requiring legislation to implement. NSDM 346 concludes:

In both these alternatives, the government would establish policy, standards, and regulations, would assist the private sector by making government-developed cryptographic technology available for commercial application, and would promote public acceptance of the need for communications security by making the private sector aware of the nature and scope of the threat as well as the commercial availability of government-approved secure communications. Industry would apply bulk protection techniques to the communications networks and would pass the added costs on to users. (National Security Decision Memorandum 346, page 1)

NSDM 346 is the distillation of three years of aggressive policy research, technological investigation, and project deployment which concludes that the public should not be informed. President Ford and his staff, well versed in information issues through their involvement in the DCCRP, Rockefeller Committee and others viewed the protection of US telecommunications networks as one of its highest priorities. NSDM

346 charts a direct course into the future for the continuation of this policy and the ongoing protection of US telecommunication networks while refraining from revealing their vulnerability to the public directly. The brief comment in the body of the Rockefeller Report is one of the few brief acknowledgements of the problem.

Conclusions

In the course of exploring telecommunications security, the US government made a number of key determinations about the relationship between government, industry, and the public with respect to privacy and national security. First, national security trumped privacy. Policymakers were very concerned about the legal, regulatory, and political problems associated with informing the public of the vulnerability of US telecommunications networks. They decided that the breadth of privacy and impact of technology was too poorly understood by the public; unlike the government which had actively been coming terms with the fusion of computers and telecommunications technologies. Individual privacy would be a secondary concern of telecommunications security. Second, the US government was in a unique position to lead telecommunications security projects because of its virtual monopoly on the development and deployment of cryptographic systems. During the 1970's, this was clearly true. (Bamford 1982; Bamford 2001; Singh 1999) The US government and specifically the NSA had expertise and technology that was unparalleled. Third, involving common carriers was crucial to the success of protecting US telecommunications. This conclusion posed significant challenges to policymakers because of the deregulation of the industry and the infrastructural security of AT&T's wireline infrastructure. Because of the urgent nature of US telecommunications security, the US government had to approach AT&T initially. It also realized that the changing nature of the

industry would require them to approach other carriers and reassure them that AT&T's prior interaction with the government was not due to favoritism, but because of AT&T's dominant technological and architectural position.

This new research invites a wide range of questions. How did the Carter Administration view the telecommunications security problem? Records indicate that it too was concerned by the situation and accepted many of the premises of the Ford Administration but modified or ignored others. The OTP was an important contributor to telecommunications security policy but was abolished during the Carter Administration. Is the NTIA, its successor agency the dual heir to the telecommunications security management entity described by Ford Administration documents and the Office of Information Policy? It meets many of the key criteria laid out in their policy research. With respect to privacy, how did the federal government employ the rhetoric of privacy to secure US telecommunications? Clearly, initial federal privacy focused on securing the massive amount of information that thanks to computers and networking technology were available to eavesdroppers. Limiting disclosure and mandating data encryption protects privacy but more importantly for policy makers in the Ford Administration, limits access to potentially damaging information about the nation and its citizens. My research into the Ford Administration's telecommunications security plan offers a new framework in which to examine the relationship between common carriers and the federal government in which cooperation is encouraged and demanded by the federal government outside of the oversight of the FCC. What of the FCC? The FCC is largely absent from the documentary record and when mentioned is viewed as more of an impediment or hurdle to traverse. Nonetheless, the Ford Administration is keen to maintain a level playing field in the common carrier market despite the deployment of

new technology and regulations. Finally, the ongoing role of technology is one worthy of further examination. What role if any did telecommunications security have in the adoption of fiber optics and digital switches? Both technologies increased the difficulty and cost of eavesdropping and may have been deemed useful to telecommunications security policy makers. Encryption technology has also been a bone of contention with the clipper chip debate and the emergence of PGP in the 1990's.

Telecommunications security and privacy continue to be an issue to the present day. Since 9/11, the federal government has focused on the new threat of terrorism made more virulent through their use of information and communications technologies. This situation is similar to the threat faced by the Ford Administration in August 1974. President Ford and Vice President Rockefeller were thoroughly familiar with privacy and telecommunications security issues through their work on various governmental committees. To them, the Soviet eavesdropping threat and the openness and vulnerability of the US telecommunications network was an urgent problem. The Ford Administration first secured governmental communications through a combination of privacy advocacy and technology adoption within the federal government. Then it began to work with the common carriers to expand security to include the private sector. All of these efforts were performed without addressing the telecommunications security issue to the public. Indeed, the public was purposely kept out of the loop for fear of the political and economic chaos that might ensue from a general panic caused by such revelations. Privacy was the public cover story for telecommunications security in an era where the public mistrusted the federal government and especially the military and intelligence communities in the wake of the Watergate scandal, the Vietnam War, and CIA activities in the US. The Ford administration believed that despite

public distrust it nevertheless had to take urgent, decisive action to secure US telecommunications from the threat of Soviet eavesdropping.

Works Cited

Annual Report of the Privacy Protection Study Commission, 6/76. Folder: Privacy Protection Study Commission-Annual Report, Box 103, Philip Buchen Files, GRFL.

Bamford, James. Body of Secrets : Anatomy of the Ultra-Secret National Security Agency : From the Cold War through the Dawn of a New Century. 1st ed. New York: Doubleday, 2001.

---. The Puzzle Palace : A Report on America's Most Secret Agency. Boston: Houghton Mifflin, 1982.

Meeting with Domestic Council on Privacy from Geoff Shepard. Folder: Privacy-Meeting with the Vice President 2/26/74, Box 12, Philip Buchen Files, GRFL.

Memo from Brent Scowcroft and Jim Cannon to the President, 1/6/77. Folder: National Security-Intelligence (18), Box 32, Presidential Handwriting File, GRFL.

Memo from Charles Joyce to Gordon Moe, 11/26/74. Folder: Telecommunications-Duckpins, Box 102, U.S. National Security Council Institutional Files, GRFL.

Memo from Jim Connor to the President, 1/12/77. Folder: National Security-Intelligence (18), Box 32, Presidential Handwriting File, GRFL.

Memo from Ken Cole to President Nixon, 1/24/74. Folder: Establishment of Privacy, Box 12, Philip Buchen Files, GRFL.

National Information Policy Report, 9/1/76. Folder: Privacy-National Information Policy Report (1), Box 56, Philip Buchen Files, GRFL.

"National Security Decision Memorandum 266." 8/16/2007

<<http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm266a.htm>>.

"National Security Decision Memorandum 296, page 1." 8/16/2007

<<http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm296a.htm>>.

"National Security Decision Memorandum 346, page 1." 8/16/2007

<<http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm346a.htm>>.

"National Security Decision Memorandums (NSDM) [Ford Administration, 1974-77]."

8/16/2007 <<http://www.fas.org/irp/offdocs/nsdm-ford/index.html>>.

Point Paper, 8/28/76. Folder: Telecommunication Panel-Meetings (1), Box 102, U.S. National Security Council Institutional Files, GRFL.

Policy Issues and Associated Legal and Regulatory Factors Involved in Implementing Multichannel Radio Protection, 7/7/76. Folder: Telecommunications Panel-Meetings (1), Box 102, U.S. National Security Council Institutional Files, GRFL.

Privacy Initial Department and Agency Recommendations. Folder: Privacy Initial Department and Agency Recommendations, Box 12, Philip Buchen Files, GRFL.

Proposed Action Plan for the Domestic Council Committee on the Right of Privacy, 3/13/74. Folder: Privacy Organization, Box 12, Philip Buchen Files, GRFL.

Report of the Special Task Group on Telecommunication Organization, 12/1/76. Folder:
National Security-Intelligence (18), Box 32, Presidential Handwriting File, GRFL.

Report to the President by the Commission on CIA Activities within the United States. Folder:
Intelligence-Rockefeller Commission Report: Final (1), Box 7, Richard Cheney Files,
GRFL, 1975.

Richard Nixon: Address on the State of the Union Delivered Before a Joint Session of the
Congress. 8/16/2007 <<http://www.presidency.ucsb.edu/ws/index.php?pid=4327>>.

"Rockefeller Commission Report." 8/16/2007 <<http://history-matters.com/archive/church/rockcomm/contents.htm>>.

Rockefeller Commission Report: Working Copy. Folder: Intelligence-Rockefeller Commission
Report: Working Copy of Part 1, 6/4/75, Box 57, James E. Connor Files, GRFL.

Singh, Simon. The Code Book. New York: Anchor Books, 1999.