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

By John Laprise

Ph.D. Candidate, Department of Media, Technology & Society
School of Communication, Northwestern University
2400 Archbury Lane 2E
Park Ridge, Illinois 60068

j-laprise@northwestern.edu

This paper was made possible through a generous research grant from the Rockefeller Archive Center and I thank all of the superior archivists with whom I worked.

Introduction

In June 1975, the Rockefeller Commission released its final report on Central Intelligence Agency (CIA) activities within the United States. Established by President Gerald Ford in January 1975, The Commission's report investigated and exposed a variety of illegal surveillance activities perpetrated by the CIA within the United States and in violation of its charter. Tucked into a small section discussing foreign intelligence threats was a passage addressing the vulnerability of domestic 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.[1]

The Rockefeller Commission had significantly weakened this section from an earlier draft at the behest of the intelligence community and the White House. Initially, the Commission had detailed a far more serious and technologically advanced threat posed by Soviet espionage:

> 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.[2]

The Ford Administration was fully aware of the scope and gravity of this threat. President Ford 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 previously led then President Nixon's Domestic Council Committee on the Right of Privacy (DCCRP). As chairman of the DCCRP, Ford led a far-ranging examination of the impact of computer and telecommunications technologies on US society. The DCCRP observed that these two technologies were converging due to rapid innovation and potentially posed a threat to individual privacy.

During the three years of his presidency, Ford issued four NSDMs on the security of US telecommunications, more than any other president. 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 about its citizens.[3] In the course of this process, the Ford Administration developed the concept of "Information Policy" for the first time. The actions of the Ford Administration are a watershed in US information policy. Both Ford and then his Vice President Nelson Rockefeller would lead the DCCRP and learn about the potential of information and communication technology. Ford and Rockefeller were also deeply involved in the crafting of US national security policy with respect to telecommunications security. This cross-pollinating work shaped the technological vision of the Ford White House by connecting telecommunications and computers. When Ford learned of Soviet eavesdropping on US telecommunications from the National Security Council (NSC), he understood the significant threat to US national security it posed. Such a capability would allow the USSR access to

valuable information collected by the US government on US citizens, businesses and organizations. 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.

The Ford Administration approached the problem of telecommunications security and information policy in a considered manner, mobilizing the NSC, National Security Agency (NSA), Office of Telecommunications Policy (OTP), and DCCRP. It addressed both issues of open and secret policy and specifically chose to exclude organizations such as the Federal Communications Commission (FCC), which had authority over public telecommunications policy to maintain secrecy. The NSC, NSA, and OTP functioned well to develop and deploy telecommunications security strategy. The DCCRP was unaware, with the exception of those members that sat in multiple organizations, of the parallel policy discussions that were taking place in secure conference rooms. In the end, these parallel tracks arrived at similar solutions to manage information policy, secret and public.

The successful response of these organizations to the telecommunications security and information policy challenges before them is attributable to the urgency and importance that the Ford Administration attached to them. Ford issued four NSDMs over a three-year span on the topic of telecommunications security, a singular event in the history of the presidency. The White House perceived the threat to be real and significant. They applied all of their resources to address the problem. The centralized decision making process led to limited scrutiny and opposition to the plan. Telecommunications providers had little choice than to cooperate with the US government, their largest client. Legally, the NSC was operating in an area in which the law had little to say. Having established the president's authority in this area, the policy making

occurred without any legal constraints. The greatest problem facing the whole process stems from the decision to exclude Congress and the FCC from the policy making process. The security measures discussed and implemented by the NSC clearly had repercussions on the public telecommunications marketplace, but Ford decided that this information could not be disclosed to the public, as public trust in government had already been damaged by the Watergate scandal.

The work of the Ford Administration had profound implications for US information policy. The subsequent Carter administration was left with a telecommunication security program which they continued to develop, leading to the creation of the National Security Telecommunications and Advisory Committee (NSTAC) during the Reagan Administration. The work of the Ford Administration also instrumentally shaped the Federal Intelligence Surveillance Act (FISA), passed during the Carter Administration and a contentious legal hurdle during the second Bush Administration to the present day.

The source material for this case comes from open materials available at the Ford Presidential library and the Rockefeller Archive Center. Given the sensitivity of the topic, it comes as a surprise that these materials are declassified. This case also indirectly employs one classified document, NSDM 338, which I reconstructed from other materials. Such uncertainty always accompanies work such as this and the role of the researcher in such situations is to minimize it. An example of this is my search for the NSA's testimony to the Rockefeller Commission. While I was able to establish a date, time, and the identity of the witnesses, I also discovered that the Commission intentionally took no notes from the briefing.[4]

The case follows a parallel structure, first exploring the more public work of the DCCRP beginning during the Nixon Administration, briefly looking at the relevant work of the

Rockefeller Commission and then concluding with the secret work of the NSC during the Ford Administration. It ends on Ford's last full day in office and shows how the White House's information and information security policies aligned and fused, though unbeknownst to all but a handful of senior policy makers.

Prelude: The Domestic Council Committee on the Right of Privacy

President Nixon formed the Domestic Council Committee on the Right of Privacy (DCCRP) in 1974 and assigned Vice President Ford as chairman. Nixon formed this committee based on growing public fears of "Big Brother"-style information control and management. In his 1974 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."[5]

These brief sentences convey the thinking of Nixon's assistant for Domestic Affairs, Kenneth Cole. In a January 1974 memo, Cole suggested to Nixon that individuals own their own personal information and that the business of society is conducted smoothly when this privacy is protected. New communications and computer technologies had greatly improved information sharing but also made information protection more difficult. He advocated that government should define and protect privacy in the face of technological change. In this articulation of privacy, Cole specifically limited the notion of individual privacy by asserting that it did <u>not</u> provide protection from overriding government responsibilities in areas such as criminal intelligence and national security.[6]

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	1. Legality and relevance 2. Technology 3. Pervasiveness	1. Individual right to discover information collection 2. Individual requirements 3. SSNs
Storage of Information	1. Security 2. Facilities	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	1. Misuse 2. Organizational	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 (OMB), Office of Telecommunications Policy (OTP), Office of Consumer Affairs, and the Domestic Council (DC). Nixon and Cole had invited these organizations to the table because of their intensive capturing, analysis and storage of personal 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.[7] As in other areas of the Nixon White House, the president and his advisors maintained tight control over policy.

The DCCRP's draft action plan of March 1974 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 reflected the privacy issues that Cole had previously articulated to Nixon. Short-term projects included restricting the use of social security numbers and protecting statistical data, IRS taxpayer data, Federal civilian data, uniformed military personnel data, and federal contractor and grantee data. Long-term projects included developing state and local statutes, strengthening the Fair Credit Reporting Act, and implementing a code of fair information practice for the private sector.[8] The broad membership of the DCCRP was a reflection of the ambition and scope of these projects and the pervasiveness of government data use.

By July 1974, the DCCRP under Ford's leadership had examined a variety of initiatives and had decided to go ahead with the implementation of proposals in fourteen areas.

Table 2: DCCRP Proposed Privacy Initiatives

Federal Data Processing and Data Systems Procurement	Develop and promulgate privacy guidelines
Computer System and Network Security	Development of security standards
Consumer Transactions	Consumer privacy rights
Cable Television Systems	Prohibit cable systems from collecting user data
Federal Mail Lists	Individual right to avoid federal mailing lists
IRS Taxpayer Data	Securing IRS data
Notice of Rights of Data Subjects	Informing consumers of the ramifications of providing information to the government
Electronic Funds Transfer Systems	Consumer privacy in electronic funds transfers
Individual Access to Federal Records	Right of individual to personal information collected by the government
Military Surveillance of Political Activities	Protect individuals from military surveillance of their political and personal activities
Federal Employees' Rights	Protect the information of federal employees
Parent/Student Access to Education Records	Protection of academic records
Individuals' Financial Records Maintained by banks	Protect individual privacy at financial institutions from government intrusion
Fair Credit Reporting Act	Protection of individual commercial records

These initiatives placed the weight of law and protection on the side of the individual citizen. The cable television system initiative would make it illegal for system operators to

collect or disseminate data from subscribers without their express permission. Likewise, fair credit reporting protections were much stronger, requiring the credit agency to notify individuals whenever any negative event was going to be applied to their credit history and allowing time for them to dispute it. Consumers would also have to be informed whenever they were subject to a credit report and credit agencies had to obtain their approval to issue any such report. The initiatives proposed by the DCCRP were strongly consumer-centric and made the individual the final arbiter of their personal information.[9]

Ford pronounced that this program of initiatives met with Nixon's goal of actionable items in a short period of time. Ford adjourned the DCCRP with the intention of reconvening in September. In the meantime, he instructed the DCCRP to begin implementation of these initiatives across the government. He further ordered that the DCCRP should monitor executive and legislative activities that might impact privacy and continue to coordinate with state and municipal officials. Finally, he also announced that the National Science Foundation's Office of Science and Technology Policy had agreed to take responsibility for long-range privacy projects.[10]

The unfolding Watergate scandal, followed by President Nixon's resignation in August 1974, left many initiatives in stasis as attention and resources were first focused on the potential impeachment and then the reconstitution of the White House under President Ford. Ford, now president, continued to make personal privacy a priority and did not neglect the DCCRP. Shortly after assuming the presidency, Ford directed that the DCCRP be temporarily put under the direction of the Domestic Council until a new Vice President was sworn in whereupon he would take up direction of the DCCRP. Nelson Rockefeller was appointed by Ford to the role of Vice President and was approved by the Senate in December 1974.[11]

Before Rockefeller could be sworn in, the task of the DCCRP grew explosively. By October 1974, the DCCRP had identified seven additional initiatives to begin work on.[12] This explosion of new privacy issues may have in part contributed to Rockefeller's attitude upon taking over leadership of the DCCRP. Rockefeller suggested in January 1975, that Ford add a privacy section to his State of the Union address and that the DCCRP be renamed the Domestic Council Committee on Privacy and Information Policy. While the first suggestion was adopted, the second was problematic for the White House. By expanding the purview of the DCCRP, the White House believed that the expanded entity would create turf battles between executive agencies which each had their own vision of information policy.[13] The DCCRP pursued an alternative option to begin examining the whole concept of information policy.

The DCCRP continued making progress on privacy issues throughout 1975. Ongoing conversations between Rockefeller and the DCCRP led them to the conclusion that the Federal government lacked a conceptual framework for information as well as any mechanism to coordinate any kind of policy on the subject.[14] To examine the idea more critically, the DCCRP convened a Roundtable on Privacy and Information Policy in September 1975 to examine the expanding sphere of issues interlinked with privacy and information policy. In December 1975, Rockefeller once again brought the DCCRP's concerns about information policy to Ford's attention. In the memo, Rockefeller noted that the Federal Government's information policy was created piecemeal by many different agencies. He asserted that the United States was moving towards a post-industrial information-based society and that it was essential that the Federal government begin to develop analytical frameworks and a unified information policy. This time he asked Ford to discuss information policy in his State of the Union Address. But unlike in the

previous year, he sought the reconstitution of the DCCRP as the Committee on Privacy and Information Policy (CPIP).[15]

Ford responded again by including an information policy section in the State of the Union Address. He did not authorize the reconstitution of the DCCRP. Rather, he directed the DCCRP and Rockefeller at its head to produce a report on information policy consisting of: a list of information policy issues relevant to federal policymakers; a status report on the ongoing information policy studies occurring across the government, and policy recommendations based upon this information. The DCCRP was further instructed to work closely with all federal agencies that had responsibilities formulating information policy. This report was to be completed and presented to the president by September 1, 1976.[16]

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.[17] 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. [18]

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 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.[19]

In September 1976, Rockefeller presented an action memo based upon the DCCRP's recommendations. The first item was the creation of an OIP to begin implementation of the report's recommendations. Rockefeller felt that this was best accomplished either within the OTP or as a temporary adjunct of the OTP. Ford assented to the latter. Second, the DCCRP was not funded for the 1977 fiscal year and its work on privacy issues was ongoing. Rockefeller

suggested and Ford agreed that the DCCRP's responsibilities and portfolio be temporarily handed over to the OTP until such time as an OIP was existent.[20]

The Other Hat: The Rockefeller Commission

While Vice President Rockefeller was leading the DCCRP forward on privacy and information policy, he also was leading the Rockefeller Commission's investigation of the CIA. As chairman of the Commission on CIA Activities within the United States (also known as the Rockefeller Commission), he became aware of the threat posed by Soviet surveillance as the commission gathered information. The commission's original mandate stemmed from President Ford's January 1975 order to examine whether the CIA had violated the privacy of US citizens and had participated in the assassination of foreign leaders in the aftermath of the Watergate scandal. While the report focused on these questions, testimony from CIA, NSA, and FBI representatives provided the commission with the unsettling knowledge that Soviet Union was eavesdropping on U.S. telecommunications networks. The U.S.S.R. was also capable of evaluating these calls and culling data from them through the use of computers. In June 1975, the Commission asserted in its final report that the protection of 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.[21]

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. During its six-month existence, the Rockefeller Commission acquired an understanding of electronic surveillance and became more aware of the vulnerability of US telecommunications networks.[22]

It was not easy for the Commission to obtain information on foreign surveillance activities within the U.S. On April 7, 1974, the commission heard testimony from the representatives of the NSA including its director, Lt. General Lew Allen, regarding Soviet signals intelligence efforts directed against the United States. The testimony was so sensitive that that their presentation was not recorded.[23] As of April 29, 1975, neither the FBI nor the CIA could offer contributions "suitable" for publication.[24] The President's Foreign Intelligence Advisory Board (PFIAB) commented on the U.S. domestic counter intelligence problem by noting that there were an ever increasing number of Soviet agents within the U.S. The PFIAB went on to note that Soviet efforts were not limited to HUMINT (human intelligence) but also SIGINT (signals intelligence) which was collected through various technical means and then analyzed by computer.[25]

The issue of size and technical means were hotly debated topics between the NSC and the Rockefeller Commission. The initial draft identified Soviet intelligence manpower at 2,000,000. Further consultation with the intelligence community reduced that to 1,000,000 and then 500,000 as the committee wanted to have a defensible number so as not to undermine the report's credibility. General Brent Scowcroft, Ford's National Security Advisor, and Secretary of State Henry Kissinger successfully argued that the wording of the final report should avoid mentioning computers and microwave communications.[26]

Following the release of the report, the deputy director of the OTP, John Eger, issued a cautionary memo regarding the report's disclosure of Soviet telephone espionage and suggesting that the OTP, NSC, and DCCRP form an interagency group to examine the issue. Ford and Rockefeller agreed but limited the DCCRP's participation to its chairman, Rockefeller.[27] Days later, the memo was withdrawn without having been seen by General White House Counsel Thomas Keller. James Connor, Ford's staff secretary, informed the OTP that the NSC was responsible for the situation. Connor further told the OTP that it should stay out of this policy area unless asked by the NSC.[28] The White House was intent on keeping Soviet espionage, computers, microwave transmitters, and telephone espionage out of the public eye even as the DCCRP was moving to consider information policy, and for good reason.

Out of the Public Eye: The NSC and DUCK PINS

Since the fateful information policy discussion between Cole and Nixon, the White House asserted that national security concerns superseded the protections afforded by personal privacy. Protecting citizens' personal information from the US government and private industry was secondary to protecting such information from the Cold War threat of Soviet eavesdropping and capture of personal information. The NSC feared that the Soviets would use personal information to suborn U.S citizens to act as agents, as was discovered by the Rockefeller Commission. Following Ford's inauguration in August 1974, the NSC informed the president that the nation's telecommunications systems were insecure and that the Soviet Union was intercepting US telecommunications. Telecommunications security would preoccupy the Ford Administration throughout its three-year existence, issuing four NSDMs on the topic.

Table 3: 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 15 August 1974, instructing James Schlesinger, Secretary of Defense that "immediate defensive steps be taken" to combat the potential for Soviet interception of wireless communications in the Washington DC area, i.e., satellite and microwave signals. NSDM 266 placed the Department of Defense (DoD) and the Office of Telecommunications Policy (OTP) in charge of this effort, which in the short term would move threatened US government communications to traditional wireline connections and in the long term would either develop secure wireless communications or expand wired connectivity. In addition, Ford informed the State Department, Office of Management and Budget, and Central Intelligence Agency of this plan.[29]

The DoD's short-term plan to secure US telecommunications in the Washington DC area was code-named DUCK PINS. This plan involved transferring sensitive government telecommunications traffic to wireline networks. DUCK PINS immediately began to ruffle feathers. Since 1974, the Federal Communications Commission had been deregulating AT&T's long-distance telephone monopoly to allow new companies such as MCI to compete. Relatively inexpensive microwave towers and satellites enabled MCI and other AT&T competitors to provide telecommunications services but NSDM 266 pronounced them vulnerable to Soviet eavesdropping. Since only AT&T had a large, secure and costly wireline infrastructure, it was

the immediate beneficiary of DUCK PINS, as it was the only carrier that could immediately offer the wireline services demanded by NSDM 266.[30]

The situation was also problematic for the General Services Administration (GSA) which was in the process of bidding out government telecommunications circuits between Washington DC and New York City in November 1974. The NSC understood that AT&T's competitors would submit competitive bids to wrest lucrative government business away from AT&T. The competitors' networks would be based upon insecure microwave architecture and would fail to meet the new requirements for secure governmental communications in NSDM 266. The GSA could not award them contracts, but could not tell them why. The GSA either had to delay or cancel the procurement or reallocate telecommunications service to eliminate the initial requirement. DUCK PINS had the potential to undercut deregulation through the secret adoption of telecommunications security measures and parameters.[31]

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. Prior to deregulation, this would have been accomplished through discussions between the federal government and AT&T. With deregulation, such discussions would have to take place with all long-distance carriers, including AT&T. If the government excluded the other carriers from the discussions, the government would have to explain its actions and publicly reveal the vulnerability of the US telecommunications infrastructure, a politically unacceptable outcome. Alternately, the US government could selectively discuss the situation and work with some telecommunications companies, but this entailed the same risk of favoritism.

One potential solution to this problem 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 they served. The NSC recognized that evaluating data systems and 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) to secure telephone communications 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 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 remain out of the public eye, in spite of the potential for publicity during the implementation of PRM.[32]

In August 1976, the Telecommunications Panel discussed a point paper examining the government's role in providing cryptographic systems and ensuring their integrity and security. Integrity and security were crucial to protecting US military, diplomatic, economic, and technological interests. Secondarily, the government would implement cryptographic systems to protect US citizens' 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 NSA, with a budget in excess of $1 billion, was responsible for protecting US government communications systems and decoding the signals of foreign governments.[33] The NSC also envisioned that a portion of the crypto key 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 advocated maintaining a complete US government monopoly on cryptographic materials and systems. It provided no evidence that cryptographic systems were to be used in an offensive manner and that the government's participation was due solely to the expertise that resided in such places as the National Security Agency.[34]

Cooperation with the common carriers became an ongoing theme of DUCK PINS. A July 1976 paper made recommendations on the implementation of multichannel radio protection that set out clear positions about the interrelationship of government, business, and the public. The paper advocated 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 the regulatory and judicial issues that would arise. Voluntary cooperation, the paper noted, would require the establishment of standards and well-defined procurement practices. It also emphasized 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 early planning of DUCK PINS because of its technological and infrastructural advantages.[35]

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 the US government's efforts to protect privacy and would be skeptical about the new regulatory and legal mechanisms 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 government create an industry advisory committee to keep all carriers 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 could 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.

Hidden from the Public Eye: the NSC and NSDM 338

NSDM 338 "Further Improvements in Telecommunications Security," issued in September 1976, remains classified.[36] 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 NSC assigned the Task Group 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.[37]

Noting that the government had already taken steps to protect critical governmental information, the report went on to say that government had an important role in preserving national communications security, as it was the repository for cryptographic expertise and provided the standards and policies that enabled the continuing function of a nationally integrated telephone system. The report emphasized 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 suggested two ways for the government to protect communications which echoed the thoughts and concerns of Joyce and Moe in 1975. The government could mandate a program by requiring the cooperation of telecommunications carriers, but this would require significant government intervention into the market and 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 reporting to the president; and designation of an existing organization in the Executive branch 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 observations 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 by the public as a military or intelligence arm of the government so that it will receive public support, but at the same time it 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 findings mirrored those of the Privacy Commission's call for an Office of Information Policy; 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.[38]

Choosing to Remain out of the Public Eye: Ford and the NSC

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 a technical assessment of US capabilities to protect telecommunications.[39] 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 cited 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 identified a number of advantages. Private organizations, once warned, would take independent measures to protect information. Public disclosure would put the administration's efforts in the "right perspective." At the time there was 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 included generating anti-Soviet sentiment and creating a panic leading to a headlong rush for more security than current technology was able to provide. Scowcroft and Cannon went 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 emphasized 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.[40] In the end, President Ford agreed to implement private sector protection, but chose not to make the telecommunications situation public. He further authorized the creation of a joint committee comprised of members of the NSC and the Domestic Council, and chaired by Vice President Rockefeller, to continue to work on telecommunications security issues.

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 was prefaced by an acknowledgement that microwave radio was insecure and easy to intercept.[41] It went on to relate that Washington DC government microwave communications had been transferred 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. The OTP had developed a deployment plan for these systems for these three cities and the rest of the nation. NSDM 346 further announced the formation of a joint committee chaired by the Vice President and tasked with deciding whether

to encourage private sector cooperation by requiring secure communications in government communications, creating standards and working with the common carriers; or to mandate a protection scheme throughout the national network which would have required legislation to implement. NSDM 346 concluded:

> 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.[42]

NSDM 346 was the distillation of three years of aggressive policy research, technological investigation, and project deployment which concluded that the public should not be informed. President Ford and his staff, well versed in information issues through their involvement in the DCCRP, Rockefeller Commission and others viewed the protection of US telecommunications networks as one of its highest priorities. NSDM 346 charted a direct course into the future for the continuation of this policy and the ongoing protection of US telecommunication networks while refraining from revealing US vulnerability to the public. The brief comment in the body of the Rockefeller Report is one of the few acknowledgements of the problem.

Analysis

This case study interweaves three subcases: the DCCRP, the Rockefeller Commission, and the telecommunications security work of the NSC. These cases overlap chronologically and thematically to explain the origins of federal information policy and look at the issue from an open, semi-open, and closed perspective. In all three subcases, the federal government acted in

an ad hoc manner to establish committees, commissions, and working groups to deal with pressing issues of information policy and security with varying degrees of success. One common factor that drove all three organizations forward was the initiative provided by President Ford and Vice President Rockefeller. Both men had a deep appreciation for the importance of computers and telecommunications networks born out of their early work on privacy with the DCCRP. This knowledge advanced telecommunications security policy and refocused the DCCRP from the issue of privacy to the broader issue of information policy. The Rockefeller Commission appears to have accidentally stumbled into the threats being addressed by the NSC and revealed them to the public. Only the efforts of National Security Advisor Scowcroft and Secretary of State Kissinger limited the diffusion of knowledge regarding the foreign surveillance threat. Rockefeller cooperated in this by steering the Commission away from this topic and towards its stated objective of examining CIA misdeeds. Rockefeller also acted as a gatekeeper between the NSC and the DCCRP to coordinate the creation of information policy.

The DCCRP's formation by Nixon to address privacy concerns was momentous. Nixon formed the DCCRP by bringing together representatives from federal agencies that held and analyzed large volumes of personal information. Under Ford and Rockefeller's leadership, many initiatives were completed to secure personal information held by the government. However, the DCCRP's initiatives that called upon the private sector to voluntarily protect personal information, such as credit and medical histories, went unheeded. The DCCRP was able to support Congress in the passing of the landmark Privacy Act of 1974, but the DCCRP's greatest successes on the issue of privacy were within the federal government and within participating agencies.

Throughout 1975 and especially in the latter half of the year, the DCCRP's orientation changed from privacy to a focus on information policy. This was in part due to the ongoing work and research of the DCCRP. However, it also coincides with the publication of the Rockefeller Commission Report and the implementation of DUCK PINS. The DCCRP's efforts to formulate privacy policy were strongly influenced by Rockefeller's activities in all three efforts.

The revelations contained in the Rockefeller Commission regarding telecommunications security were little more than a footnote, but prompted some of the most heated discussions over content within the White House. It seems clear from the documentary record that the Commission examined domestic counterintelligence efforts for the sake of completeness. The Commission was taken aback by the revelations of the NSA and the PFIAB regarding Soviet surveillance efforts and did not resist Scowcroft and Kissinger's efforts to play down the information in the final report. This may also mark the point at which Rockefeller became aware of the work of the NSC on telecommunications security, which was top secret and highly compartmentalized. When Ford issued NSDM 266, Rockefeller was not yet Vice President. By June 1975, when both NSDM 296 and the Rockefeller Commission report emerge, Rockefeller was communicating about telecommunications security policy with the NSC, but was not on the distribution list for NSDM 296. The speed with which the DCCRP changed its focus to investigate information policy and the subsequent inclusion and mention of Rockefeller in NSC telecommunications security documents indicates that Rockefeller may have also been taken by surprise. President Ford's support for Rockefeller's plan to change the DCCRP's focus to information policy indicates that Ford and Rockefeller were sharing information in the second half of 1975.

The NSC's response to the telecommunications security problem was direct and swift. President Ford issued NSDM 266 almost immediately upon taking office and pressed the NSC with a flurry of subsequent NSDMs. Ford had been concerned about personal privacy since chairing the DCCRP under Nixon. Ford perceived Soviet surveillance to be a grave threat. The NSC acted in concert with few agencies to bring DUCK PINS to fruition. It included the NSA because the protection of federal communications was one of the NSA's prime missions and because the NSA had unique expertise in the field. The NSC also involved the DoD as it was the NSA's parent organization. The DoD also contained the Defense Communications Agency, which had experience developing, deploying and maintaining secure communications networks. The OTP was involved almost by default. By charter federal telecommunications policy was the OTP's responsibility, but almost from the entity's creation during the Nixon Administration it struggled to establish itself, fighting numerous turf battles with the Departments of Commerce and Defense as well as the FCC. Even though the White House had created it, the OTP rarely enjoyed presidential support for its policies and initiatives, and it would be abolished by the Carter Administration.

The NSC's interactions with civilian agencies were even more authoritative. It all but ordered the GSA to comply with new telecommunications security requirements. The NSC and the president were extremely wary of Congress and the FCC for fear that any information provided to them would swiftly become headline news. In the post-Watergate environment, with multiple investigations like the Rockefeller Commission occurring, Ford and the NSC were acutely aware that the public trust in the federal government was at historic lows. The public would be alarmed to learn that U.S. telecommunications systems were vulnerable to interception by the Soviets and by extension the federal government. They believed that the public would

refuse to accept assigning the White House's most secret intelligence agency to protect the vulnerable public phone calls.

The origin of information policy in the federal government centers on President Ford and Vice President Rockefeller. Both men learned about the breadth of personal information held by the federal government through their chairmanship of the DCCRP. Presidential succession and the Rockefeller Commission exposed them to the national security implications of this situation. One reason why they were successful in pushing forward their information policy agenda was their similar visions and the lack of any opposition. Nixon created the DCCRP and Ford created the Rockefeller Commission and both were responsible to the President. While their work and findings were read by Congress and the public, it was consumed by the White House. The DCCRP, the Rockefeller Commission, and the NSC were beholden to the President and designed to him.

The lack of external oversight over Ford and Rockefeller with respect to information policy and security is startling but unsurprising. The policies they advanced all regulated the actions of the executive branch which they oversaw and were generally quite successful. Indeed, problems emerged when policy moved beyond the executive branch, such as the lack of private cooperation with the DCCRP and DUCK PIN's regulatory challenges. Internal squabbles, such as OTP's turf struggles, were quickly and easily dealt with.

Conclusions

In the course of exploring telecommunications security, Ford and Rockefeller 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 U.S. 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 to terms with the fusion of computers and telecommunications technologies. Individual privacy was secondary to telecommunications security and information policy. Second, it was imperative that the federal government develop a sound, cogent information policy. The U.S. economy was moving towards an information-based economy and society and the government needed to begin considering relevant policies. Third, the NSA 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.[43] The federal government and specifically the NSA had expertise and technology that was unparalleled. Finally, the NSC needed to involve common carriers to insure 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 NSC had to approach AT&T initially. The NSC 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? The Ford Administration had set in motion a range of telecommunications and information policy plans and gave responsibility for their completion to the Carter Administration. A preliminary analysis of the records indicates that the Carter Administration was concerned by the situation and accepted many of the premises of the

Ford Administration but modified or ignored others. Ford had designated the scorned OTP as heir to telecommunications security and information policy, but the Carter Administration abolished the OTP. How did this alter the path of federal policy? Is the NTIA, the OTP's 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? Initial federal privacy policy focused on securing the massive amount of information held by the government on the public. The work of the DCCRP and the NSC approached information security from different directions. The DCCRP was concerned with possible government misuse of information while the NSC sought to eliminate foreign acquisition of such information. 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 and information policy offers new insights into the origins of U.S. information policy. It provides new examples of the relationship between common carriers and the federal government in which cooperation is encouraged and demanded by the federal government without the oversight or knowledge 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. The FCC was concerned with regulating broadcast and common carriers. Nonetheless, the Ford Administration was 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.

The DCCRP's initial goal of insuring the privacy of citizens in an information age quickly expanded into a full-fledged examination of information policy. As Rockefeller became aware of not just the necessity of protecting federally held data from not only the federal government but also from foreign governments, privacy necessarily expanded. By the end of the Ford Administration, policymakers agreed that a single entity needed to be created, empowered to create, implement, and manage information policy. The unswerving commitment of Ford and Rockefeller to the creation of information policy drove this agenda forward, informed by research bodies like the DCCRP and the Rockefeller Commission.

Telecommunications security and information policy 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 leading the DCCRP and the Rockefeller Commission. 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 had to take urgent, decisive action to secure US telecommunications from the threat of Soviet eavesdropping.

[1] 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, Gerald R. Ford Presidential Library (GRFL), 1975.

[2] 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.

[3] "National Security Decision Memorandum 266." 8/16/2007 <http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm266a.htm>.

[4] Minutes, David Belin, April 7, 1975, folder 338.1, box 17, series 19, RG 26 Nelson A. Rockefeller (NAR) Vice Presidential (NAR) , Rockefeller Family Archives (RFC), Rockefeller Archive Center (RAC).

[5] 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>.

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

[7] 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.

[8] 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.

[9] Memorandum: DCCRP Agenda and Materials for July 10, 1974 meeting, Folder Right of Privacy, Domestic Council Committee, Box 229, Robert Hartmann Files, Ford Vice Presidential Papers (FVPP), GRFL.

[10] Memorandum: DCCRP Agenda and Materials for July 10, 1974 meeting, Folder Right of Privacy, Domestic Council Committee, Box 229, Robert Hartmann Files, Ford Vice Presidential Papers (FVPP), GRFL.

[11] Memo Buchen to Ford, 8/27/74, Folder: FG: DCCRP, Box 12, Presidential Handwriting File, GRFL.

[12] Memo Metz to Department and Agency Liasons DCCRP, 10/23/74, Folder: DCCRP(2), Box 27, Edward C. Schmults Files, GRFL.

[13] Memo Parsons to Cannon, 1/13/75, Folder: DCCRP (2), Box 27, Edward C. Schmults Files, GRFL.

[14] Memo Rodgers to Rockefeller, 8/25/75, Folder: Privacy DCC General 4/75-1/76, Box 13, DC-Richard D. Parsons Files, GRFL.

[15] Memo Rockefeller to Ford, 12/17/75, Folder 18, Box 18, Series 18, RG 26, NAR, RFC, RAC.

[16] Memo Ford to Rockefeller, 3/8/76, Folder 35, Box 18, Series 18, RG 26, NAR, RFC, RAC.

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

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

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

[20] Memo Rockefeller to Ford, 9/14/76, Folder: FG: DCCRP, Box 12, Presidential Handwriting File, GRFL.

[21] Report to the President by the Commission on CIA Activities within the United States. (1)

[22] Report to the President by the Commission on CIA Activities within the United States. (1)

[23] Minutes, David Belin, April 7, 1975, folder 338.1, box 17, series 19, RG 26, NAR, RFC, RAC.

[24] Memo Wallison to Rockefeller, 4/29/75, Folder 389, Box 17, Series 19, RG 26, RFC, RAC.

[25] PFIAB Report "The Counterintelligence Problem in the United States", 5/8/75,folder 384, box 16, series 19, RG 26, NAR, RFC, RAC.

[26] Memo Howe to Rockefeller, 5/31/75, folder 62, box 14, series 19, RG 26, NAR, RFC, RAC.

[27] Memo Wallison to Connor, 7/3/75, folder UT 1-3, box 198, series 3, NAR, RFC, RAC.

[28] Action Memo Scowcroft to Rockefeller, Buchen, Connor, O'Neill, 6/30/75, folder June 1975 (4), Box 36, James Connor Staff Secretary, GRFL.

[29] "National Security Decision Memorandum 266." 8/16/2007 <http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm266a.htm>.

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

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

[32] "National Security Decision Memorandum 296, page 1." 8/16/2007 <http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm296a.htm>.

[33] Report, Folder 400, Box 18, Series 19, RG 26, NAR, RFC, RAC.

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

[35] 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.

[36] "National Security Decision Memorandums (NSDM) [Ford Administration, 1974-77]." 8/16/2007 <http://www.fas.org/irp/offdocs/nsdm-ford/index.html>.

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

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

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

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

[41] "National Security Decision Memorandum 346, page 1." 8/16/2007 <http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm346a.htm>.

[42] "National Security Decision Memorandum 346, page 1." 8/16/2007 <http://www.ford.utexas.edu/library/document/nsdmnssm/nsdm346a.htm>.

[43] 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.

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