

---

# Appendixes

## APPENDIX A

# Letters of Request

### NINETY-FIFTH CONGRESS

PETER W. RODINO, JR. (N.J.), CHAIRMAN

JACK BROOKS, TEX.  
ROBERT W. KASTENMEIER, WIS.  
DON EDWARDS, CALIF.  
JOHN CONYERS, JR., MICH.  
JOSHUA EILBERG, PA.  
WALTER FLOWERS, ALA.  
JAMES R. MANN, S.C.  
JOHN P. SEIBERLING, OHIO  
GEORGE E. DANIELSON, CALIF.  
ROBERT F. DRINAN, MASS.  
BARBARA JORDAN, TEX.  
ELIZABETH HOLTZMAN, N.Y.  
ROMANO L. MAZZOLI, KY.  
WILLIAM J. HUGHES, N.J.  
SAM B. HALL, JR., TEX.  
LAMAR GUDGER, N.C.  
HAROLD L. VOLKMER, MO.  
HERBERT E. HARRIS II, VA.  
JIM SANTINI, NEV.  
ALLEN E. ERTSEL, PA.  
BILLY LEE EVANS, GA.  
ANTHONY C. BEILENSEN, CALIF.

ROBERT MCCLORY, ILL.  
TOM RAILSBACK, ILL.  
CHARLES E. WIGGINS, CALIF.  
HAMILTON FISH, JR., N.Y.  
M. CALDWELL BUTLER, VA.  
WILLIAM S. COHEN, MAINE  
CARLOS J. MOORHEAD, CALIF.  
JOHN M. ASHBROOK, OHIO  
HENRY J. HYDE, ILL.  
THOMAS N. KINDRESS, OHIO  
HAROLD S. SAWYER, MICH.

## Congress of the United States Committee on the Judiciary

House of Representatives

Washington, D.C. 20515

Telephone: 202-225-3951

GENERAL COUNSEL:  
ALAN A. PARKER

STAFF DIRECTOR:  
GARNER J. CLINE

ASSOCIATE COUNSEL:  
FRANKLIN G. POLK

September 12, 1977

Senator Edward M. Kennedy  
Chairman of the Board  
Office of Technology Assessment  
119 D Street, N.E.  
Washington, D. C. 20510

Dear Senator Kennedy:

The House Committee on the Judiciary, Sub - Committee on civil and Constitutional Rights, pursuant to its legislative and oversight responsibilities over the FBI, is currently undertaking a study of the FBI's criminal justice information systems and related matters. The Committee has been interested in this area for some time, most recently in connection with the Bureau's request to the Department of Justice for new equipment and message switching capability for its National Crime Information Center. The Subcommittee has focused its attention on the systems' cost-effectiveness, efficiency, security and privacy protections. In addition, the larger issue of what should be the role of the federal government in this exchange of information by and for local law enforcement agencies has been raised.

In view of the technical complexity of nationwide computerized information and telecommunications systems, the Committee would like to have the assistance of the Office of Technology Assessment. In particular, we believe that OTA's assistance would be most helpful in addressing the following issues:

1. Evaluation of the Bureau's NCIC system in terms of benefits to the users, accuracy of the data, speed, efficiency and reliability.
2. The Department of Justice is currently developing a proposal with both short and long range plans for the future of NCIC, the FBI's role in law enforcement telecommunications systems and message

switching generally. An analysis of the proposal is needed in terms of the issues raised above, i.e.:

does the proposal call for implementation of the newest and best technology available (Is that technology necessary to carry out the functions described in the proposal?);

does it provide for appropriate privacy and security measures and safeguards for constitutional rights and civil liberties; .

does it take into account the needs of its primary users, the states, on an ongoing basis;

does it or should it, provide for systematic audits of the system, both internal and external, announced and unannounced;

will it improve the speed of response and reduce the current downtime levels, both of which are cited as problems by some users and outside computer experts (Are these in fact serious problems?) ;

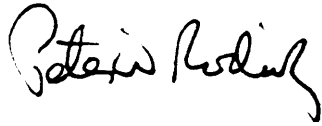
does it strike the appropriate balance between state and federal control of this system, keeping in mind that the Subcommittee leans toward the least intrusive federal (FBI) involvement possible, consistent with efficient operation of the system.

These questions and issues are not meant to be all-inclusive. For example, in a report prepared for the Subcommittee by the Scientists' Institute for Public Information, a copy of which is enclosed, additional problems were cited, and suggestions for change were made. Your evaluation of those problems and suggestions would also shed much light on this inquiry. Finally, your answers to all of these questions may, in turn, lead you to identify and assess alternatives, which would be useful to the Subcommittee's study.

Senator Edward M. Kennedy  
September 12, 1977  
Page 3

---

Your assistance in this matter would be greatly appreciated. We look forward to hearing from you in the near future.



PETER W. RODINO, JR.  
CHAIRMAN

Sincerely,



Don Edwards  
Chairman  
Subcommittee on Civil and  
Constitutional Rights

SCIENTISTS INSTITUTE FOR PUBLIC INFORMATION  
355 Lexington Avenue  
New York, N.Y. 10017  
(212) 661-9110

**TASK FORCE ON SCIENCE AND TECHNOLOGY  
IN THE CRIMINAL JUSTICE SYSTEM  
Project on Criminal Justice Information Systems**

**Report on inspection and briefing at the National Crime Information Center,  
July 12, 1977, and follow-up, August 2, 1977.**

Prepared by:

John J. Kennedy, Esq.  
Director, Criminal Justice Task  
Force  
August 3, 1977

On July 12, 1977, a group representing SIPI'S Task Force on Science and Technology in the Criminal Justice System performed an on-site inspection of the National Crime Information Center at Hoover FBI Headquarters in Washington, D.C. A briefing was conducted by Raymond J. Young, Assistant Section Chief, NCIC, and a lengthy question period followed. The SIPI group consisted of the following computer scientists: Daniel D. McCracken, Task Force Chairperson, and Vice-President of the Association for Computing Machinery; Joseph Weizenbaum, Professor of Computer Science, Massachusetts Institute of Technology; and Dr. Myron Uretsky, Director, Management Decision Laboratory, New York University Graduate School of Business Administration. They

were accompanied by John J. Kennedy, Esq., Task Force Director, and Alan McGowan, President of SIPI. After a preliminary report of that visit was prepared, Mr. Kennedy returned on August 2, 1977 to meet with Frank B. Buell, Section Chief, NCIC, and with Mr. Young, to give the FBI an opportunity to respond to the preliminary report. As a result of that follow-up visit, some corrections were made in the preliminary report. The thirteen points discussed below represent some problem areas of the NCIC as they appeared to the SIPI group as a result of these visits.

1. There is no regular auditing of NCIC data and procedures by a relatively independent auditing authority. Department of Justice

Regulations place the responsibility for the auditing of Computerized Criminal History data on each state to perform its own audit. The NCIC Advisory Policy Board statement of October 20, 1976, also mandates systematic audits on the part of the states with respect to CCH data. There are no Regulations at all which mandate any audit of non-CCH data. Therefore, neither the FBI nor any other agency except the submitting state audits what goes into the system and how it goes in. The FBI only scrutinizes state systems when it is invited to do so by that state, or when the FBI suspects wrongdoing on the part of employees of the system. The FBI does point out errors in procedure and obvious data errors that come to its attention. However, the opinion of the Task Force was that independent auditing, both announced and unannounced, as in the case of bank audits, is crucial to maintaining the accuracy and integrity of data, and to ensure that adequate computer management practices and safeguards are being followed. For example, the rate of inaccurate records can best be determined by independent audit, but at the present time such figures for the system as a whole are unavailable. Finally, one Task Force member felt that the "friendly" relations between the local law enforcement agencies and the FBI, and the desire to keep those relations friendly, militated against a system where one part was truly looking over another part in a critical way.

2. There has been no in-depth evaluation of the actual benefits of NCIC either performed by the states or by the FBI despite 10 years of operation. Except for a number of highly dramatic incidents that are reported on occasion to indicate that NCIC works, there have been no studies, evaluations, or reports which give hard data on the benefits that have resulted to criminal justice as a result of NCIC. For example, what use does the criminal justice community make of NCIC data, and how does this improve criminal justice efforts? The actual benefits of NCIC still remain in the area of surmise, rather than demonstrated results.

3. For such a vast system, containing over 6½ million records, with 250,000 transactions per day, the hit ratio was not demonstrated to be impressive. The system has about 1,000 hits per day, of which 50% were for stolen vehicles, 20-25 % for wanted persons, and the rest scattered over the other six non-CCH files. There was no reliable data available for the CCH hit ratio. Without studies of the context of the hits, even in cases involving the "hot" files there is no proven demonstration of the significance of these hits. There is insufficient available proof of whether an extremely rapid response, which NCIC is designed to provide, is of such vital significance in a great proportion of these 1,000 daily hits. In addition, all of the information obtained through NCIC could be obtained elsewhere, admittedly, by a less rapid manner, since all the data is kept at the state level. There are other sources of criminal justice information in addition to this state maintained data. For example, there is a stolen car list maintained by a consortium of insurance companies which the FBI admits is in some respects more accurate and up-to-date than the NCIC stolen vehicle file which relies on state-supplied information. Perhaps the NLETS system, in the case of much interstate information, is an adequate, alternative communication device. The maintenance of the huge NCIC system, growing every year, may be subject to question when there is no demonstration that the 1,000 daily hits provide a significant benefit to law enforcement, and that comparable information may be available by other means, at cheaper cost, and with less significant problems involving intergovernmental relations.
4. The downtime of the system was viewed as excessive. There are about 30 hours per month of unscheduled downtime, and about 2-3 hours per month of scheduled downtime. On 7/12/77 the system had operated for eight straight days without downtime, but has had other occasions when the system was down for as long as 11 hours. It requires a minimum of 45 minutes to restart the system after downtime; it requires a cold start; and the down-

time is more due to hardware than software. Although the system has 94% uptime, the Task Force said that this would be an unacceptable record in most commercial enterprises. If such downtime existed in a bank or insurance company, it would be a situation requiring immediate corrective action. The FBI plans to request additional funds for some costly equipment upgrading, designed, in part, to solve this problem of downtime.

5. "Expungement" from the system does not mean true expungement of a record. Back-up tapes and a log are necessarily maintained by NCIC for system reliability purposes. This is a necessary precaution common in computer systems. However, since back-up tapes and a log are maintained, "expungement" ("cancellation," "clear") from NCIC really means that the expunged data is not available on-line, but does exist on tapes that are kept at FBI Headquarters. Expungement from NCIC can occur due to the fact that the initial entry was incorrect, among other reasons, but even this sort of expungement would still entail a record being maintained by the FBI, even of the erroneous data, kept on back-up tapes. The problem of expunged data does not involve insignificant numbers. For example, in a recent ten-day period, there were cancels and clears on 17,000 stolen vehicles, 2,500 CCH files, 1,000 "articles," 2,000 license plates, 6,200 wanted or missing persons, and 1,800 guns. There are a variety of reasons for these clears and cancels, but some percentage of them involve errors that put people into the files who never belonged there in the first place. Yet, these records will be maintained on NCIC back-up tapes.
6. There have been at least eight lawsuits resulting from the use of NCIC data, one of which was directed against the Section Chief of NCIC. These suits can result from false arrest, unlawful search and seizure, or other improper practices. One of the side benefits of not fully expunging data is to defend law enforcement personnel from lawsuits by pointing to data that had previously been maintained in NCIC at one time, which may have given "probable cause" for the law enforcement action that the lawsuit arose over.
7. The FBI admits that there has been poor disposition reporting by the courts. This means that arrest records remain in the system without updating of the outcome of that arrest. The arrest records do not drop out of CCH even if no disposition is ever reported. Although there are limits on the dissemination of arrest data to non-criminal justice agencies, nonetheless, data on stale arrests are not removed from the system. One Task Force member suggested that arrest data in CCH be removed unless there is prompt disposition reporting. As the system is now operated, a person will have an arrest record maintained indefinitely in CCH whether or not he is ever convicted in a court.
8. NCIC requires a cumbersome correction and updating procedure. When an entering agency corrects an error or wishes to update a record, it must transmit that data to the central state control terminal, for further transmission to NCIC central headquarters in Washington. However, in addition to the data having to pass through several different steps for correction, this procedure doesn't provide for complete correction or updating of NCIC data. For example, assume that Florida has made an input of incorrect data to NCIC, or certain data that it has input is now stale. Suppose that this is CCH data concerning John Doe. If Michigan makes an inquiry to NCIC about John Doe, Michigan will receive either incorrect or stale data. Further assume that Florida then corrects or updates John Doe's record. Nonetheless, Michigan is still in possession of the stale or incorrect data on John Doe, and unless Michigan makes another information request on John Doe, Michigan will not receive the correct and up-to-date data through NCIC. It is not possible for Florida to directly update or correct Michigan's record on John Doe through NCIC. Under current procedures, even after Florida has carried out the process of correction on-line, nevertheless, the FBI still must inform Michigan through the mails that there has been an expungement

on John Doe. There is no mail correction or updating on non-CCH files. Local law enforcement agencies are advised not to act on old NCIC hits. Only fresh hits are viewed as being adequate, and even then, the person who gets the hit must confirm this information with the entering state by another means than NCIC.

9. The procedures for the verification and certification of data by the states does not prevent at least some stale and incorrect data from being in NCIC at any given time. Every six months the FBI sends to each state either a print-out or tapes of the data that that state has submitted to NCIC that is still being maintained in the system. The state must certify that this data is correct. However, unless the state at that point takes affirmative action to correct the data sent back to it by the FBI, the data will remain in the system. That is, the state certification procedure makes the implied assumption that the data, as it is already being maintained, is correct and up-to-date. One Task Force member suggested that an alternative method would be for NCIC to periodically start with a clean slate, and have each state submit all data at that point which it could certify as correct and up-to-date. By the former method, there is an implied assumption that the data in the system is correct and up-to-date. By the latter method, no such assumption is made, and a greater burden of verification and certification is placed on each state. A second problem is that the certification procedure is carried out only every six months. This can leave a substantial time gap in the correction of records which allows a certain percentage of bad data to remain in the system during that time gap. Finally, the sanction for a state which certifies data incorrectly can include being cut-off from the system, which can also be applied in cases of improper practices of other kinds. However, because the sanction of cut-off is viewed as draconian, it is applied sparingly. No state has ever been cut off from the hot files. Only one local law enforcement agency has ever been cut off from NCIC, and that was an action taken by the State of Ohio. Three other states in the past have been tem-

porarily cut-off from the CCH file due to reorganization of procedures in those states, but have since been restored to CCH. In a system where the only effective sanction is cut-off, the problem of enforcing procedures is a delicate one.

10. People are not informed when a CCH record is maintained on them. They do have the right to check their own file through a cumbersome process and the payment of fees in some cases, but figures were not available on the number of people who actually do check. There was some feeling expressed by Task Force members that people should be informed periodically if a record is being maintained concerning them. Address information of the people on which records are maintained appears on the fingerprint cards related to the record in CCH.
11. There are serious security and privacy considerations when between 6,600 and 7,000 terminals can access NCIC nationwide. As the number of terminals increase, with a potential of 45,000 local, state, and Federal criminal justice use terminals, the opportunities for abuse also increase. As long as someone can either gain unauthorized access themselves, or gain indirect access through an authorized user, a system containing sensitive data is open to abuse.
12. Despite nearly six years of operation, only 11 states are participating in the CCH portion of NCIC by providing some input, and of these, only 2 are fully participating in the sense of providing input of all arrest records. FBI Director Clarence M. Kelley, in an April 15, 1977 memo to Attorney General Bell, reiterated his previous request to terminate FBI participation in the CCH portion of NCIC. Director Kelley's reasons repeated his previously advanced reasons such as excessive cost of the system, lack of participation by the states, and the absence of authority for a "message-switching" capability which caused duplication of data at both the state and Federal levels. CCH records make up about 1670 of the total number of records in NCIC, yet even the head of the agency that manages the system questions the efficacy of this portion of it, and calls for the end of this portion.



13. In a May 19, 1977 memo, Peter F. Flaherty, Deputy Attorney General, wrote to Director Kelley that the Justice Department had undertaken a study to see if "interstate message switching should be authorized for the CCH program. " Message switching would entail keeping CCH data on Federal and multi-state offenders centrally maintained by the FBI, but having data on single-state offenders (about 70% of the total) maintained by the states. The FBI would keep a "pointer" file which would direct an inquiry from State X to the proper state where that CCH record was being maintained, and the capability would exist for State X to query State Y through the NCIC. The FBI would supply the facilities for a state to inquire over FBI maintained lines to each of the other states. However,

this raises at least two questions. One, with direct state-to-state access, through the FBI, would there be a tremendous increase in the amount of criminal justice information that would be available on-line? For example, California's CLETS system submits only about 10% of its criminal history data to CCH, determined by the gravity of the offense, residence of the defendant, and other factors. However, with direct access, would the entire CLETS system be available to other states? The Task Force felt that as interconnection increases, problem areas multiply. Two, in this electronic context, due to the design of this central switching system, would this mean that the FBI would control the flow of ever-increasing amounts of criminal justice information throughout the country?

## Task Force Members

Daniel D. McCracken; Ossining, New York (Chairperson)  
Vice-President, Association for Computing Machinery  
Consultant, and author of 14 books in computing field

Joseph Weizenbaum  
Professor of Computer Science, MIT  
Former member, Secretary's Advisory Committee on  
Automated Personal Data System, Dept. of HEW  
Author, *Computer Power and human Reason*  
(W. H. Freeman & Co., 1976)

Douglas H. Haden  
Assistant Professor of Computer Science  
New Mexico State University  
Author, *Social Effects of Computer Use and Misuse*  
(John Wiley & Sons, 1976)

Dr. Myron Uretsky  
Director, Management Decision Laboratory  
NYU Graduate School of Business Administration

Paul Armer; San Francisco, California  
On-Line Business Systems, Inc.  
Formerly at the Center for Advanced Study in the  
Behavioral Sciences, Stanford, California

Dr. Jerry M. Rosenberg  
Professor of Management  
Polytechnic Institute of New York  
Author, *The Death of Privacy*  
(Random House, 1969)

Dr. Robert R. J. Gallati  
Northeastern University  
Criminal Justice Program  
Formerly, Director of the New York State Identification  
and Intelligence System

Jeremiah Gutman, Esq; New York, NY  
Levy, Gutman, Goldberg & Kaplan  
Chairman, ACLU Privacy Committee

Ronald E. Yank, Esq.; San Francisco, California  
Carroll, Burdick, and McDonough  
Counsel, Peace Officers Research Association  
of California

Anthony Ralston  
Chairman, Department of Computer Science  
State University of New York at Buffalo  
Past-President, American Federation of Information  
Processing Societies (AFIPS)

Dr. Rein Turn; Redondo Beach, California  
Staff Engineer, Software Analysis and Evaluation Dept.  
Defense and Space Systems Group of TRW, Inc.

Professor Lance J. Hoffman  
George Washington University  
Department of Electrical Engineering and  
Computer Science

Dr. Norman H. White  
Assistant Professor of Computer Applications  
NYU Graduate School of Business Administration

JAMES O. EASTLAND, MI SS., CHAIRMAN

JOHN L. McCLELLAN, ARK. STROM THURMOND, S.C.  
EDWARD M. KENNEDY, MASS. CHARLES MCC. MATHIAS, JR., MD.  
BIRCH BAYH, IND. WILLIAM L. SCOTT, VA.  
ROBERT C. BYRD, W. VA. PAUL LAXALT, NEV.  
JAMES ABOUREZK, S. DAK. ORRIN G. HATCH, UTAH  
JAMES B. ALLEN, ALA. MALCOLM WALLOP, WYO.  
JOSEPH R. BIDEN, JR., DEL.  
JOHN C. CULVER, IOWA  
HOWARD M. METZENBAUM, OHIO  
DENNIS DE CONCINI, ARIZ.

FRANCIS C. ROSENBERGER  
CHIEF COUNSEL AND STAFF DIRECTOR

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, D.C. 20510

February 15, 1978

Dr. Russell W. Peterson  
Director  
Office of Technology Assessment  
Congress of the United States  
Washington D. C. 20510

Dear Dr. Peterson:

It is our understanding that the Office of Technology Assessment is now engaged in a preliminary analysis of the National Crime Information Center in response to a request for an assessment which you received from Chairman Rodino of the House Judiciary Committee and Chairman Edwards of the Subcommittee on Civil and Constitutional Rights.

As Chairman of the Senate Judiciary Committee and as Chairmen of the Subcommittee on Administrative Practice and Procedure and the Subcommittee on the Constitution, we join in this request for a full scale assessment and evaluation of the NCIC. In view of the present and proposed role of the Federal Government in the operation and management of this exchange of information for local law enforcement agencies, we believe there is an urgent need for an evaluation of the NCIC for: (1) its benefits to the users and to taxpayers in terms of the accuracy of its data, its speed, efficiency and reliability; and (2) its consequences for effective protection of constitutional rights in the administration of justice.

The Department of Justice is currently considering various plans for updating and expanding NCIC which would include returning the computerized criminal histories (CCH) records of NCIC to the states which have already put them into the system and operating a central message switching center for local and state police agencies when they request information from other jurisdictions. This would result in a major expansion of this nation-wide system, with implications for the right of states to control local law enforcement and to develop related information systems in light of their own statutes governing privacy and freedom of information. Justice Department plans also raise major constitutional rights problems of privacy, confidentiality, security, due process and civil liberties where the technology may interact with administrative and judicial policy.

The Senate Judiciary Committee has conducted hearings and considered legislation on these issues for some several Congresses without the benefit of a thorough evaluation of exactly what information is in the system, and who needs it and why.

Especially interested in these issues is the Subcommittee on Administrative Practice and Procedure whose oversight jurisdiction encompasses both the substantive and procedural internal practices and procedures of federal agencies. The Subcommittee is strongly in favor of a comprehensive and efficient system of law enforcement, and joins with the Justice Department in seeking this goal. However, the importance of assuring a citizen's constitutional rights of due process, privacy, and civil liberties is also of prime concern.

The Subcommittee on the Constitution also has a particular interest in the NCIC. Over the past several years it has held several hearings on the issues raised by criminal information storage and retrieval systems and the various constitutional and privacy concerns presented by them. The Subcommittee has recently engaged in an exchange of correspondence with the Attorney General on the Department's plans and intentions for NCIC.

We are, in addition, concerned with the issue of Federal control over State information, and how that issue will be dealt with in the proposed system. If the long term social consequences, **beneficial** as well as adverse, of this law enforcement information system are to be fully identified for Congress, we believe several areas need to be fully explored by your current working group.

First, with respect to the issue of the impact of the interrelationship of the many information policies which govern the administrative practices of Federal and State agencies which use or are affected by NCIC--particularly by the computerized criminal history files, **(CCH)** ---

a. An analysis from the perspective of the right of privacy, freedom of information, due process rights and civil liberties in general should be made with respect to the above question.

b. An analysis of the Federal vs. State roles with respect to the handling of the information in the system: i.e., which person or entity will control what data in the new NCIC system, and which person or entity will be held accountable for the quality of information in the system--and by what method this will be done.

c. An analysis should be made of the effectiveness of the policies, both for the present and future NCIC system, with respect to expungement of irrelevant, old, or inaccurate data. For instance, how would the standards for such a process be set and maintained and/or changed, if necessary? Who or what entity would be responsible for the accuracy of all records in the system? How would this be audited or reviewed in light of the right of privacy, due process and civil liberties concerns?

Second, there should be an analysis of any efforts being made to identify and address "flagging" as a potential civil liberties problem.

Thirdly, we believe that an evaluation of the efficiency of NCIC and of any proposed technological changes should encompass the effect of those changes on all other Federal users of NCIC files. This would include, for instance, the Department of Agriculture, the Veteran's Administration, Customs and the other Treasury Department Bureaus, the State Department, the Secret Service, and other interested Federal agencies. In connection with this issue, we would also like to know whether the Department of Justice plans for NCIC have considered possible alternative future relationships between those federal agencies and CCH records and NCIC data banks and computerized files.

What would be the effect on individual constitutional rights and other guarantees if the present NCIC relationships are altered? How would an enlarged system such as proposed, compare with the present system in terms of privacy, due process and civil liberties safeguards? Would certain rearrangements of NCIC tend to magnify or extend some undesirable features of the Federal use of NCIC? On the other hand, would certain rearrangements make it more difficult or costly for some agencies to use and support NCIC to the detriment of their programs and of the rights of citizens?

The fourth area which concerns us as Members of the Judiciary Committee is the relationship of NCIC programs, operations and controls to the Federal and State Judiciary. Could proposals to change NCIC tend in the long-run to fester or threaten the constitutional separation of the Judiciary from the Executive

branch and the Legislature, at all levels of government? Would pending proposals to change NCIC tend to promote or retard the ability of State judicial officials to make the most efficient use of data systems in order to protect the rights of citizens involved in the judicial process? We are not familiar with any studies that have dealt directly with this question.

Fifth, the ramifications of Federal message switching, when incorporated into such a law enforcement information system as NCIC, need to be thoroughly explored for its impact on the rights of the individual in our society, and on the powers of the States, (and on the ability of private enterprise to compete with the Federal Government). We realize that message switching is a common technique which is useful in a great variety of government and private information programs. However, there are aspects of some of the current NCIC proposals in this area which need further study in light of civil liberties and other concerns which have been often voiced by the public and press and emphasized in Congress.


Last, but not least, we have yet to see an evaluation of the NCIC concept, that is, of whether or not an NCIC-type system is the most efficient way to accomplish the law enforcement goals desired, and whether or not we actually need a nation-wide system such as that proposed. Should private enterprise play a greater role in providing services? To what extent should the Federal government compete with private industry? An OTA assessment should, in view of your statutory mission, include an analysis of alternatives to NCIC. For instance, would an alternative arrangement be more effective in achieving our goals? How effective, for instance, would it be to develop a system based on regional data banks? Under various alternatives, what would happen to political rights and privileges of citizens?

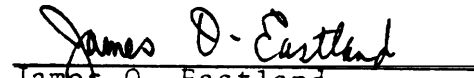
We believe Congress will benefit from OTA'S assessment of NCIC. This system represents the first and most important nation-wide use of computer and telecommunications technology to link federal, state and local governments, and to apply the technology to serious law enforcement and criminal justice problems of concern to our entire society. Many of the issues involved in NCIC are those common to any such Federal-State information system..

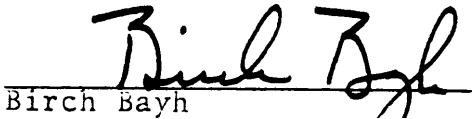
Dr. Russell W. Peterson  
page five

The Federal and State governments will spend millions of dollars to develop fully the NCIC and the data programs and technology which feed and support it. It is difficult, if not impossible, to reverse the effects of misjudgment or poor planning in such programs. Therefore we believe it is important to ask hard questions now and to have them resolved than to have them fester as social and legislative issues for years to come simply because governments and taxpayers have let themselves become indentured to costly and complex technology.

Sincerely,

  
James Abourezk  
Chairman  
Subcommittee on Administrative  
Practice and Procedure

  
James O. Eastland  
Chairman  
Senate Judiciary Committee

  
Birch Bayh  
Chairman  
Subcommittee on the Constitution

RICHARDSON PREYER, N.C., CHAIRMAN  
LEO J. RYAN, CALIF.  
JOHN E. MOSS, CALIF.  
MICHAEL HARRINGTON, MASS.  
LES ASPIN, WIS.  
PETER H. KOSTMAYER, PA.  
THEODORE S. WEISS, N.Y.  
BARBARA JORDAN, TEX.

PAUL N. McCLOSKEY, JR., CALIF.  
J. DANFORTH QUAYLE, IND.  
JOHN N. ERLINGER, ILL.

225-3741

NINETY-FIFTH CONGRESS  
CONGRESS OF THE UNITED STATES

House of Representatives

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS  
SUBCOMMITTEE  
OF THE  
COMMITTEE ON GOVERNMENT OPERATIONS

RAYBURN HOUSE OFFICE BUILDING, Room B-349-B-C  
WASHINGTON, D.C. 20513

September 19, 1977

Mr. Daniel V. DeSimone  
Acting Director  
Office of Technology Assessment  
Senate Annex #3  
Washington, D.C. 20510

Dear Mr. DeSimone:

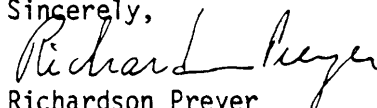
As Chairman of the Subcommittee on Government Information and Individual Rights of the House Government Operations Committee, I wish to confirm the previous request made by this subcommittee on September 8, 1976 for the assistance of the Office of Technology Assessment, and to seek your help in further projects of concern. The subcommittee has assignments involving the field of computer technology and other means of electronic communications which flow from our legislative jurisdiction, particularly from the mandates of the Privacy Act of 1974 and the Freedom of Information Act.

The earlier request, a copy of which is attached, was in connection with the need for technical support for the Congress in its review of Executive agency proposals to alter or establish information systems. That OTA can perform an important service in this area is clear from its assessment of the proposed Tax Administration System. OTA involvement on a more regular basis would, of course, be most desirable. In this regard, I and my staff would welcome the opportunity to discuss this matter with you.

Of equal, if not greater importance is the subcommittee's concern over the impact of technological advances on the development of government information programs in general. Our interests in this area would, I believe, be best served through listing the subcommittee as a sponsor for the upcoming OTA exploration of the need for a government-wide policy on computers and telecommunications. This sponsorship would afford ample opportunity for subcommittee input on those aspects of the exploration study which relate to our jurisdiction.

Thank you for your consideration and continued cooperation.

Sincerely,



Richardson Preyer  
Chairman



NINETY-FIFTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS  
SUBCOMMITTEE  
OF THE  
COMMITTEE ON GOVERNMENT OPERATIONS  
RAYBURN HOUSE OFFICE BUILDING, ROOM B-349-B-C  
WASHINGTON, D.C. 20315

September 8, 1976

Emilio Q. Daddario, Director  
Office of Technology Assessment  
119 D Street, N.E.  
Washington, D.C. 20510

Dear Mr. Daddario:

The Subcommittee on Government Information and Individual Rights of the House Government Operations Committee, which I chair, has assignments involving the field of computer technology and other means of electronic communications which flow from our legislative jurisdiction, particularly from the mandates of the Privacy Act of 1974 and the Freedom of Information Act.

The Privacy Act of 1974 requires the departments and agencies to make provisions in their information systems for observing privacy, confidentiality, security of systems, and certain due process rights of the individual with respect to personal records, and for recognizing certain principles of good administration in agency record-keeping. Reports to Congress are made for each major alteration or new information system, indicating how these administrative values are incorporated in the data system and in the information practices.

Although the Act requires reports to Congress, it does not provide for the logistical scientific support needed for a qualitative review of these reports. The proposals are usually drawn by computer scientists in technological terms and frequently give only pro forma recognition to those operational areas of concern to Congress when it passed the Privacy Act. The preliminary reviews afforded them within the agencies and the Office of Management and Budget, as well as the review afforded in the appropriations process in Congress address economic and technical feasibility problems, unless the proposed data system would result in a glaring violation of individual privacy. However, the very complexities of these systems may disguise significant changes. Important administrative and constitutional values of privacy and due process may be affected by the technology as it is applied to various programs unless certain technical and administrative guarantees are established in advance.

Enilio Q. Daddario, Director  
September 8, 1976

Page Two

As new technology becomes available and existing systems are strained, billions of dollars will continue to be spent on these new or expanded data systems. Due to their size and complexity, any errors or negative impacts on individual rights in the operations of federal programs will be expensive and difficult to correct. It is important therefore that on certain vital issues the union of the technological and policy dimensions be established from the beginning, and it is not at all clear that this is currently being done or will be done in the future. I believe that effective oversight by Congress must incorporate these two elements and must result in institutionalizing it at some point in the process.

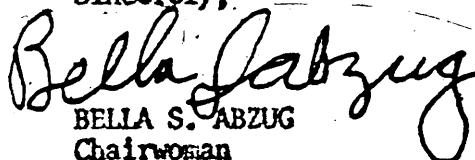
This search for the union of policy and technology seems to me to be a particularly appropriate area in which the Subcommittee might benefit from the advice and assistance of the Office of Technology Assessment. Congress sorely needs education and help in its evaluation of these scientifically-oriented systems reports, and it appears to be precisely the type of project for which the OTA is uniquely suited.

For example, the proposal for a new Tax Administration System is one such report on which the Subcommittee would welcome the advice or recommendation of the Office of Technology Assessment with respect to the adequacy of the Internal Revenue Service's stated guarantees concerning privacy and other individual rights.

I ~~and my~~ staff would welcome the opportunity to discuss with you the possibility of receiving OTA's technical assistance on a regular basis, or its advice in developing a format for the Subcommittee's routine consideration of those aspects of the agency systems reports filed with the Government Operations Committee which relate to our jurisdiction.

Your cooperation is deeply appreciated.

Sincerely,

  
BELLA S. ABZUG  
Chairwoman