

FCC 92-182

38394

RECEIVED

MAY 12 1992

FCC MAIL BRANCH

Before the  
Federal Communications Commission  
Washington, D.C. 20554

In the Matter of )  
Establishment of )  
Systems of Records )  
Exempt Under the Privacy Act )

MD Docket No. 92-92

**NOTICE OF PROPOSED RULEMAKING**

**Adopted:** April 16, 1992

**Released:** May 12, 1992

**Comment Date:** June 11, 1992

**Reply Comment Date:** June 26, 1992

By the Commission: Commissioner Quello issuing a statement.

**I. INTRODUCTION**

1. By this Notice of Proposed Rulemaking, the Commission proposes to amend section 0.561 of the Commission's Rules to exempt two new systems of records from certain provisions of the Privacy Act of 1974, 5 U.S.C. Section 552a.<sup>1</sup> The proposed two systems of records would be entitled "FCC/OIG-1, Criminal Investigative Files" and "FCC/OIG-2, General Investigative Files." The first system of records is limited to records on individuals, including present and former FCC employees, who are or have been the subjects of investigations conducted by the Office of Inspector General (OIG) in accordance with the Inspector General's authority derived from the Inspector General Act of 1978, as amended. These criminal investigations arise within the context of alleged violations of criminal laws which proscribe fraud and abuse in the execution of the Commission's programs and operations. The second system of records will contain investigative material compiled for general law enforcement purposes.<sup>2</sup>

---

1 A system of records is a group of records under an agency's control from which information is retrieved by the individual's name or by some other unique personal identifier, such as social security number. See 5 U.S.C. Section 552a(a)(5).

2 The proposed rule is typical of other federal agency rules in this area. See 16 C.F.R. Section 4.13(m); 17 C.F.R. Section 200.313.

## II. DISCUSSION

2. FCC/OIG-1. The Privacy Act allows the head of any agency to promulgate rules to exempt any system of records within the agency from certain provisions of the Privacy Act of 1974, if the system of records is maintained by any agency or component thereof which performs as its principal functions any activity pertaining to the enforcement of criminal laws, as follows:

(a) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;

(b) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or

(c) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

3. The contents of proposed system FCC/OIG-1 is limited to the information of the type described above. It will be maintained by the OIG, a component of FCC, which performs as one of its principal functions activities pertaining to the enforcement of criminal laws. The authority for the criminal law enforcement activities of the OIG is the Inspector General Act of 1978, 5 U.S.C. Appendix 3. This statute authorizes the IG to conduct criminal investigations relating to programs and operations of the FCC. In accordance with 5 U.S.C. 552a(j)(2), we propose to exempt the information maintained in this system of records from all of the provisions of the Privacy Act except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (e)(7), (e)(9), (e)(10), (e)(11) and (i).<sup>3</sup>

---

3 In general, these provisions allow the disclosure of information from systems of records pursuant to the Freedom of Information Act or pursuant to a court order, to agency employees on a "need to know" basis, to Congress, to certain agencies such as the Bureau of Census and the National Archives, and to law enforcement agencies when the information is requested by the head of such agency. Further, these provisions set forth certain administrative and accounting requirements that agencies must meet in connection with systems of records pertaining to criminal investigations.

4. In general, the disclosure of information contained in the criminal investigative files, including the names of persons or agencies to whom the information has been transmitted, would substantially compromise the effectiveness of OIG investigations. Knowledge of such investigations could enable suspects to take such action as is necessary to prevent detection of criminal activities, conceal or destroy evidence or escape prosecution. Disclosure of this information could lead to the intimidation of, or harm to, informants, witnesses, and their families, and could jeopardize the safety and well-being of investigative and related personnel and their families. The imposition of certain restrictions on the manner in which investigative information is collected, verified or retained would significantly impede the effectiveness of OIG investigatory activities and, in addition, could preclude the apprehension and successful prosecution of persons engaged in fraud or criminal activity. The exemption is needed to maintain the integrity and confidentiality of criminal investigations and to protect individuals from harm. The specific reasons for exempting this system of records are discussed below.

5. Section (c)(3) of the Privacy Act requires an agency to make the accounting of each disclosure of records available to the individual named in the record at his/her request. These accountings must state the date, nature and purpose of each disclosure of a record and the name and address of the recipient. Accounting for each disclosure would alert the subjects of an investigation to the existence of the investigation and the fact that they are subjects of the investigation. The release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation and could seriously impede or compromise the investigation, endanger the physical safety of confidential sources, witnesses, law enforcement personnel and their families and lead to the improper influencing of witnesses, the destruction of evidence or the fabrication of testimony.

6. Section (c)(4) of the Privacy Act requires an agency to inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of the Act. Since this system of records is being exempted from subsection (d) of the Act concerning access to records, this section is inapplicable to the extent that this system of records will be exempted from subsection (d) of the Act.

7. Section (d) of the Privacy Act requires an agency to permit an individual to gain access to records pertaining to him/her, to request amendment to such records, to request a review of an agency

decision not to amend such records and to contest the information contained in such records. Granting access to records in this system of records could inform the subject of an investigation of an actual or potential criminal violation, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his/her activities, of the identity of confidential sources, witnesses, and law enforcement personnel, and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an investigation, endanger the physical safety or confidential sources, witnesses, law enforcement personnel and their families, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony and disclosure investigative techniques and procedures. In addition, granting access to such information could disclose classified, security-sensitive or confidential business information and could constitute an unwarranted invasion of the personal privacy of others.

8. Section (e)(1) of the Privacy Act requires each agency to maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required by statute or by executive order of the President. The application of this provision could impair investigations and law enforcement because it is not always possible to detect the relevance or necessity of specific information in the early stages of an investigation. Relevance and necessity are often questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation, the investigator may obtain information which is incidental to the main purpose of the investigation but which may relate to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation, the investigator may obtain information concerning the violation of laws other than those which are within the scope of his/her jurisdiction. In the interest of effective law enforcement, OIG investigators should retain this information, since it can aid in establishing patterns of criminal activity and can provide valuable leads for other law enforcement agencies.

9. Section (e)(2) of the Privacy Act requires an agency to collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs. The application of this provision could impair investigations and law enforcement by alerting the subject of an investigation, thereby enabling the subject to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence or to fabricate testimony. Moreover, in certain circumstances the subject of an investigation cannot be required to provide information to investigators and information must be collected from other sources. Furthermore, it is

often necessary to collect information from sources other than the subject of the investigation to verify the accuracy of the evidence collected.

10. Section (e)(3) of the Privacy Act requires an agency to inform each person whom it asks to supply information, on a form that can be retained by the person, of the authority under which the information is sought and whether disclosure is mandatory or voluntary; of the principal purposes for which the information is intended to be used; of the routine uses which may be made of the information; and of the effects on the person, if any, of not providing all or any part of the requested information. The application of this provision could provide the subject of an investigation with substantial information about the nature of that investigation and this could interfere with the investigation. Moreover, providing such a notice to the subject of an investigation could seriously impede or compromise an undercover investigation by revealing its existence and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

11. Sections (4)(G) and (H) of the Privacy Act requires an agency to publish a Federal Register notice concerning its procedures for notifying an individual, at his/her request, if the system of records contains a record pertaining to him/her, how to gain access to such a record and how to contest its content. Since this system of records is being exempted from subsection (f) of the Act, concerning agency rules, and subsection (d) of the Act, concerning access to records, these requirements are inapplicable to the extent that this system of records will be exempted from subsection (f) and (d) of the Act. Although the system would be exempt from these requirements, the Commission has published some information concerning the availability of these procedures for records in this system because, under certain circumstances, the OIG could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records. See attached description of system of records entitled: FCC/OIG-1: Criminal Investigative Files.

12. Section (e)(4)(I) requires an agency to publish a Federal Register notice concerning the categories of sources of records in the system of records. Exemption from this provision is necessary to protect the confidentiality of the sources of information, to protect the privacy and physical safety of confidential sources and witnesses, and to avoid the disclosure of investigative techniques and procedures.

13. Section (e)(5) requires an agency to maintain its records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in making any determination about the individual. Since the Act defines "maintain" to include the collection of information, complying with this provision could prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In collecting information for criminal law enforcement purposes, it is not possible to

determine in advance what information is accurate, relevant, timely, and complete. Facts are first gathered and then placed into a logical order to prove or disprove objectively the criminal behavior of an individual. Material which may seem unrelated, irrelevant, or incomplete when collected can take on added meaning or significance as the investigation progresses. The restrictions of this provision could interfere with the preparation of a complete investigative report, thereby impeding effective law enforcement.

14. Section (e)(8) requires an agency to make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record. Complying with this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation.

15. Section (e)(12) requires that, if an agency is a recipient agency or a source agency in a matching program with a non-Federal agency, the federal agency must publish notice of the establishment or revision of such program in the Federal Register at least 30 days prior to conducting the program. At this time, this provision is not applicable to the Commission.

16. Section (f)(1) requires an agency to promulgate rules which shall establish procedures whereby an individual can be notified in response to his/her request if any system of records named by the individual contain a record pertaining to him/her. The application of this provision could impede or compromise an investigation or prosecution if the subject of an investigation were able to use such rules to learn of the existence of an investigation before it could be completed. In addition, mere notice of the fact of an investigation could inform the subject and others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Since this system would be exempt from subsection (d) of the Act, concerning access to records, the requirements of subsection (f)(2) through (5) of the Act, concerning agency rules for obtaining access to such records, are inapplicable.

17. Section (g) provides for civil remedies if an agency fails to comply with the requirements concerning access to records under subsections (d)(1) and (3) of the Act; maintenance of records under subsection (e)(5) of the Act; and any other provision of the Act, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual. Since this system of records would be exempt from subsections (c)(3) and (4), (d),(e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H) and (e)(4)(I), (e)(5), (e)(8) and (f) of the Act, the provisions of subsection (g) of the Act would be inapplicable to the extent that this system of records will be exempted from those subsections of the Act.

18. FCC/OIG-2. The Privacy Act also allows the head of any agency to promulgate rules to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I) and (f) of this section if the system of records is investigative material compiled for law enforcement purposes. The proposed FCC OIG-2 will contain investigative material compiled for law enforcement purposes and maintained by the OIG. The OIG is authorized by the Inspector General Act to conduct investigations relating to programs and operations of the Federal Communications Commission. In general, the exemption is needed to maintain the integrity and confidentiality of law enforcement investigations. The specific reasons for exempting this system of records are discussed below.

19. Section (c)(3) of the Privacy Act requires an agency to make the accounting of each disclosure of records available to the individual named in the record at his/her request. These accountings must state the date, nature and purpose of each disclosure of a record and the name and address of the recipient. Accounting for each disclosure would alert the subjects of an investigation to the existence of the investigation and the fact that they are subjects of the investigation. The release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation and could seriously impede or compromise the investigation, endanger the physical safety of confidential sources, witnesses, law enforcement personnel and their families and lead to the improper influencing of witnesses, the destruction of evidence or the fabrication of testimony.

20. Section (d) of the Privacy Act requires an agency to permit an individual to gain access to records pertaining to him/her, to request amendment to such records, to request a review of an agency decision not to amend such records and to contest the information contained in such records. Granting access to records in this system of records could inform the subject of an investigation of an actual or potential law violation, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his/her activities, of the identity of confidential sources, witnesses, and law enforcement personnel, and could provide information to enable the subject to avoid detection or apprehension. Granting access to such information could seriously impede or compromise an investigation, endanger the physical safety or confidential sources, witnesses, law enforcement personnel and their families, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony and disclosure investigative techniques and procedures. In addition, granting access to such information could disclose classified, security-sensitive or confidential business information and could constitute an unwarranted invasion of the personal privacy of others.

21. Section (e)(1) of the Privacy Act requires each agency to maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required by statute or by executive order of the President. The application of this provision could impair investigations and law enforcement because it is not always possible to detect the relevance or necessity of specific information in the early stages of an investigation. Relevance and necessity are often questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established. In addition, during the course of the investigation, the investigator may obtain information which is incidental to the main purpose of the investigation but which may relate to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated. Furthermore, during the course of the investigation, the investigator may obtain information concerning the violation of laws other than those which are within the scope of his/her jurisdiction. In the interest of effective law enforcement, OIG investigators should retain this information, since it can aid in establishing patterns of illegal activity and can provide valuable leads for other law enforcement agencies.

22. Sections (e)(4)(G) and (H) of the Privacy Act requires an agency to publish a Federal Register notice concerning its procedures for notifying an individual, at his/her request, if the system of records contains a record pertaining to him/her, how to gain access to such a record and how to contest its content. Since this system of records is being exempted from subsection (f) of the Act, concerning agency rules, and subsection (d) of the Act, concerning access to records, these requirements are inapplicable to the extent that this system of records will be exempted from subsection (f) and (d) of the Act. Although the system would be exempt from these requirements, OIG has published some information concerning the availability of these procedures for records in this system because, under certain circumstances, OIG could decide it is appropriate for an individual to have access to all or a portion of his/her records in this system of records. See attached description of system of records entitled: FCC/OIG-2: General Investigative Files.

23. Section (e)(4)(I) of the Privacy Act requires an agency to publish a Federal Register notice concerning the categories of sources of records in the system of records. Exemption from this provision is necessary to protect the confidentiality of the sources of information, to protect the privacy and physical safety of confidential sources and witnesses, and to avoid the disclosure of investigative techniques and procedures.

24. Section (f)(1) of the Privacy Act requires an agency to promulgate rules which shall establish procedures whereby an individual can be notified in response to his/her request if any system of records named by the individual contain a record pertaining to him/her. The application

of this provision could impede or compromise an investigation or prosecution if the subject of an investigation were able to use such rules to learn of the existence of an investigation before it could be completed. In addition, mere notice of the fact of an investigation could inform the subject and others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Since this system would be exempt from subsection (d) of the Act, concerning access to records, the requirements of subsection (f)(2) through (5) of the Act, concerning agency rules for obtaining access to such records, are inapplicable to the extent that this system of records will be exempted from subsection (d) of the Act.

### III. OTHER MATTERS

25. This Notice of Proposed Rulemaking is issued under the authority contained in sections 4(i) and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. sections 154(i) and 303(r), and Sections (j)(2) and (k)(2) of the Privacy Act, 5 U.S.C. Sections 552a(j)(2); (k)(2). Pursuant to applicable procedures set forth in Sections 1.415 and 1.419 of the Commission's Rules, 47 C.F.R. Sections 1.415 and 1.419, interested parties may file comments on or before June 11, 1992 and reply comments on or before June 26, 1992. To file formally in this proceeding, participants must file an original and five copies of all comments, reply comments and supporting comments. If participants want each Commissioner to receive a personal copy of their comments, an original and nine copies must be filed. Comments and reply comments should be sent to Office of the Secretary, Federal Communications Commission, Washington, D.C. 20554. Comments and reply comments will be available for public inspection during regular business hours in the Dockets Reference Room (Room 239) of the Federal Communications Commission, 1919 M Street, N.W., Washington, D.C. 20554.

26. This is a nonrestricted notice and comment rulemaking proceeding. Ex parte presentations are permitted, except during the Sunshine Agenda period, provided they are disclosed as provided in Commission rules. See generally 47 C.F.R. Sections 1.1202, 1.1203, and 1.1206(a).

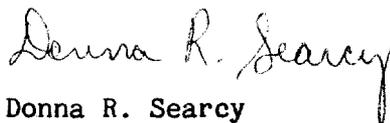
27. We certify that the Regulatory Flexibility Act of 1980 does not apply to this Rulemaking proceeding because if the proposed rule amendments are promulgated there will not be a significant economic impact on a substantial number of small entities, as defined by Section 601(3) of the Regulatory Flexibility Act. The proposed rule amendment merely exempts systems of records from certain access and disclosure requirements under the Privacy Act, and is not expected to have any economic impact. The Secretary shall send a copy of this Notice of Proposed Rulemaking, including the certification, to the Chief Counsel for Advocacy of the Small

Business Administration in accordance in the paragraph 603(c) of the Regulatory Flexibility Act, 5 U.S.C. Section 601 et seq.

**IV. ORDERING CLAUSE**

**28.** Accordingly, IT IS ORDERED, that, pursuant to Sections 4(i) and 303(r) of the Communications Act and Sections (j)(2) and (k)(2) of the Privacy Act, NOTICE OF PROPOSED RULEMAKING is hereby provided as indicated above.

FEDERAL COMMUNICATIONS COMMISSION



Donna R. Searcy  
Secretary

**APPENDIX**

**Part 0 - COMMISSION ORGANIZATION**

1. The authority citation for Part 0 continues to read as follows:

**AUTHORITY: 47 U.S.C. 154, 303 unless otherwise noted. Implement 5 U.S.C. 552, unless other noted.**

2. Section 0.561 is amended by adding two new paragraphs as follows:

Section 0.561 Exemptions.

\* \* \* \* \*

(f) System name. Criminal Investigative Files--FCC/OIG-1. Compiled for the purpose of criminal investigations. This system of records is exempt under the provisions of section (j)(2) of the Privacy Act because the records contain investigatory material compiled for criminal law enforcement purposes.

(g) System name. General Investigative Files--FCC/OIG-2. Compiled for law enforcement purposes. This system of records is exempt under the provisions of section (k)(2) of the Privacy Act because the records contain investigatory material compiled for law enforcement purposes.

**Separate Statement of  
Commissioner James H. Quello**

**RE: In the Matter of Establishment of Systems of Records Exempt Under the Privacy Act.**

I support seeking comment on what records, if any, should be exempt under the Privacy Act. I recognize the need to gather information relating to alleged wrong doings and the need to protect those who may be participating in such investigations. At the same time, caution must be exercised whenever individuals' access to information is restricted, especially when such information may affect their careers. In cases where investigations conclude no wrong doing on the part of employees, I believe individuals should have access to records, or at least be assured that the records are sealed and destroyed in a relatively short time. Maintaining records on individuals-- especially when they are found innocent -- seems inconsistent with the basic principles of justice and due process. Such records, no matter how securely maintained, always run the risk of falling into unauthorized hands and may jeopardize careers, the very concerns that prompted Congress to vote the Privacy Act. I look forward to the comments to be filed in this proceeding.