~~SECRET~~

EXHIBIT A
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN THE MATTER OF THE APPLICATION	:	
OF THE UNITED STATES FOR AN ORDER	:	
AUTHORIZING ELECTRONIC SURVEILLANCE	:	Docket Number:
OF A UNITED STATES PERSON AGENT	:	
OF A FOREIGN POWER. ~~(S)~~	:	

STANDARD MINIMIZATION PROCEDURES

Pursuant to § 101(h) of the Foreign Intelligence Surveillance Act of 1978, the following procedures have been adopted by the Attorney General, and shall be followed by the Federal Bureau of Investigation (FBI), in conducting this electronic surveillance as ordered by the Court:

Section 1 - Applicability and Scope

These procedures apply to the acquisition, retention, and dissemination of nonpublicly available communications and other information concerning unconsenting United States persons that is collected in the course of telephone, microphone, closed circuit television (CCTV), modem, facsimile, leased line and other electronic surveillance of a United States person who is an agent of a foreign power consistant with the need of the United States to obtain, produce, and disseminate foreign intelligence information. ~~(S)~~

~~SECRET~~

Classified by: Allan Kornblum, Deputy Counsel for Intelligence Operations, Office of Intelligence Policy and Review, U.S. Department of Justice
Reason: 1.5(c)
Declassify On: X1

~~SECRET~~

Section 2 - Definitions

(a) Definitions set forth in § 101 of the Foreign Intelligence Surveillance Act, including the terms "foreign intelligence information," "United States person," and others which may be used in these procedures, shall apply to these procedures. (U)

(b) As used herein "communications of a United States person," includes all communications to which a United States person is a party. "Communications concerning a United States person" includes all communications in which a United States person is discussed or mentioned, except that communications are not "communications concerning a United States person" if they reveal only publicly available information about the person. (U)

(c) When the citizenship status of a party to a communication being surveilled is unknown, and no reasonable basis exists for concluding that the party is not a United States person, it is presumed that such party is a United States person. (U)

(d) As used herein, "nonverbal information" shall include, but not be limited to, CCTV pictures as well as typewriter and machine noises. (U)

Section 3 - Acquisition

(a) Interception

The FBI may intercept all communications and nonverbal information of or concerning United States persons which are carried over wire communications lines or are acquired by electronic, mechanical, or other surveillance device authorized by Court order. The FBI may also intercept all oral communications and nonverbal information of or concerning United States persons which occur within the target premises as authorized by Court order. ~~(C)~~

(b) Verification

At the initiation of electronic surveillance, the FBI shall verify that the telephone communications lines being intercepted are the telephone lines of the target agent of a foreign power authorized by Court order. (U)

(c) Microphone and CCTV

[redacted]

(d) Recording

Electronic surveillance of the target agent of a foreign power may either be monitored contemporaneously, recorded automatically or conducted by a combination of both means. (U)

(e) Monitoring and Logging

(1) Monitoring and recording of electronic surveillance of the premises of a United States person shall be conducted by Special Agent or senior monitoring personnel except when the following situations make it impossible or impractical:

(A) no monitor is available with fluency in the language being intercepted; or

(B) specific operational, technical or security problems make it impossible. (U)

(2) In the event that all communications are acquired by automatic recording, the monitor of the automatically acquired tape will employ the same principles of logging, indexing, and using the information as if it had been acquired by a live monitor. (U)

(3) FBI personnel who monitor the electronic surveillance contemporaneously or who monitor automatically acquired information shall exercise reasonable judgment in determining

whether particular information intercepted must be minimized. (U)

(4) A permanent written record or "log" shall be maintained by personnel who contemporaneously monitor communications being surveilled or who monitor automatically acquired information; provided that identities or communications of or concerning United States persons that could not be foreign intelligence information or are not evidence of a crime which has been, is being, or is about to be committed may not be logged or summarized. Foreign intelligence information acquired in other forms, such as facsimile messages, computer modem data, or other electronically generated product, may be indexed and filed without a separate log being prepared. (S)

(5) When the identity of the United States person could not be foreign intelligence information, even though the content of the communication could be foreign intelligence information, the monitor shall not log the full name of the United States person but may use a partial name or characterization of the person. (S)

(f) Privileged Communications

[redacted]

[redacted]

(g) Nonpertinent Communications

(1) Communications of United States persons acquired in this surveillance will be the subject of continuing analysis to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(2) These categories should be established after a reasonable period of monitoring the communications of the target. (U)

[redacted]

(7) The Attorney General, or a designee, shall periodically determine that information concerning communications of or concerning United States persons that is logged or summarized meets the requirements of these procedures and the Foreign Intelligence Surveillance Act. (S)

[redacted]

(i) Known/Extended Absences

[redacted]

Section 4 - Internal Use and Retention

(a) Indexing

Logged identities of United States persons and communications of or concerning United States persons may be indexed into the general FBI indices only after the supervising case agent has determined that both the identity and the communication reasonably appear to be foreign intelligence information or are evidence of a crime which has been, is being, or is about to be committed. The identity of the United States person as recorded in the log may be minimized by striking the name or substituting a characterization for that person. Logged identities of any persons, including United States persons, will be recorded in the Electronic Surveillance Index pursuant to Title 18, United States Code, § 3504, if the

supervising case agent has determined that the identities reasonably appear to be foreign intelligence information and if they meet other indexing criteria established by the Federal Bureau of Investigation. (U)

(b) Transcription, Duplication, and Other Records

Communications or nonverbal information of or concerning United States persons may be transcribed or duplicated, and reports made of their contents only for authorized foreign intelligence, foreign counterintelligence, countersabotage and international terrorism or law enforcement purposes. (C)

(c) Foreign Intelligence Information

Intercepted communications or nonverbal information of or concerning United States persons which contain foreign intelligence information as defined in § 2(a) may be used only in foreign counterintelligence investigations or for other authorized foreign counterintelligence, countersabotage or international terrorism purposes. Foreign intelligence information which is also evidence of a crime which has been, is being, or is about to be committed, may also be used as provided in § 4(d) below. (C)

(d) Evidence of Crime Not otherwise Foreign Intellicence Information

Intercepted communications or nonverbal information of or concerning United States persons, that is acquired incidental to the collection of foreign intelligence information and contains information that is evidence of a crime which has been, is being, or is about to be committed, but which is not otherwise foreign intelligence information, may be retained or used only for the purpose of preventing the crime or enforcing the criminal law. (C)

(e) Controlled Access

Strict controls shall be placed on the storage and retrieval of intercepted communications of or concerning United States persons. Use shall be restricted to those FBI

supervisory, investigative, and clerical personnel who have a need to know such information to fulfill foreign intelligence or law enforcement responsibilities. (U)

(f) Destruction of Tapes

Tape recordings and duplicate tapes of communications or nonverbal information of or concerning United States persons shall be destroyed within a reasonable period of time following their authorized retention and use as provided above, except that: ~~(S)~~

(1) tapes containing evidence of a criminal offense will be retained until a decision is rendered by prosecutive authorities. If it is decided to prosecute, tapes will be retained until the end of the prosecution process; (U)

(2) tapes containing communications that reasonably appear to be exculpatory ("Brady") material shall be retained as if they contained evidence of a crime; (U)

(3) tapes containing privileged communications will be retained until ordered to be destroyed by the Department of Justice; and (U)

(4) tapes required to be retained by a rule of law or judicial order will be retained in accordance with the requirements of that rule or order. (U)

(g) Destruction of Information Acquired By Means Other Than Audio Recording

Information acquired by means other than audio recording, including but not limited to facsimile or computer modem interception, shall be reviewed in accordance with the standards for Internal Use and Retention set forth in these guidelines. [redacted]

Section 5 - Dissemination

(a) General Restrictions

(1) Subject to the requirements of this Section, nonpublicly available information concerning United States persons obtained from the electronic surveillance of the target agent of a foreign power may not be disseminated without the consent of the United States person involved unless the information is, or reasonably appears to be, foreign intelligence information as defined in §§ 101(e)(1) and (2) of the Foreign Intelligence Surveillance Act, or is evidence of a crime which has been, is being or is about to be committed. (U)

(2) Nonpublicly available information concerning United States persons obtained from electronic surveillance of the target agent of a foreign power which is foreign intelligence information may be disseminated within the Federal Government to officials, agencies, or components with responsibilities directly related to the information proposed to be disseminated, and, upon approval of the Attorney General, may be disseminated to a foreign government. In exigent circumstances, where Attorney General approval cannot be obtained in advance, dissemination to a foreign government may be made without such prior Attorney General approval in order to protect life or property from threatened force or violence; however, notification to the Attorney General shall be made as soon as possible after that dissemination, and shall include a description of the exigent circumstances requiring such dissemination. Information which is evidence of a crime may be disseminated to Federal, state, local, or foreign officials or agencies with law enforcement responsibility for the crime. ~~(S)~~

(b) Section 101(e)(1) Foreign Intelligence Information

Nonpublicly available information concerning United States persons obtained from the electronic surveillance of the target agent of a foreign power which is or reasonably appears to be foreign intelligence information as defined in § 101(e)(1) of the Foreign Intelligence Surveillance Act may be disseminated in a manner that identifies United States persons only for authorized foreign intelligence, foreign counterintelligence, countersabotage and international terrorism, or law enforcement purposes. (U)

(c) Section 101(e)(2) Foreign Intelligence Information

Nonpublicly available information concerning United States persons obtained from the electronic surveillance of the target agent of a foreign power which is or reasonably appears to be foreign intelligence information as defined in § 101(e)(2) of the Foreign Intelligence Surveillance Act may not be disseminated in a manner that identifies any United States person, except by general characterization, unless such person's identity is necessary to understand the information or assess its importance and may be disseminated only for authorized foreign intelligence, foreign counterintelligence, countersabotage and international terrorism, or law enforcement purposes. (U)

(d) Criminal Information

Nonpublicly available information concerning United States persons obtained from the electronic surveillance of the target agent of a foreign power which is evidence of a crime which has been, is being, or is about to be committed, but which is not or does not reasonably appear to be foreign intelligence information as defined by § 101(e) of the Foreign Intelligence Surveillance Act may be disseminated only for law enforcement purposes. Any information acquired from electronic

surveillance of the target agent of a foreign power which is disseminated for law enforcement purposes shall be accompanied by a statement that such information or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General. (U)

Janet Reno
Attorney General of the United States

9/12/97
Date