OFFICE OF GENERAL COUNSEL

MEMORANDUM FOR THE DEPUTY CHIEF OF STAFF

THRU: GC

SUBJECT: (U) SHARING OF "RAW SIGINT" THROUGH DATABASE ACCESS

(U//~~FOUO~~) You have asked us to conduct a legal review in order to set out the limits -- and the rationale associated with the limits -- on allowing personnel from other agencies access to NSA databases under the existing rules governing such access, and the advisability of changes to the Executive Order that would allow other agencies access to SIGINT databases.

(U//~~FOUO~~) We conclude that compliance with NSA's Attorney General-approved minimization procedures, which are required by Executive Order 12333 and are rooted in Fourth Amendment privacy protections, constrains NSA from granting to employees of other intelligence agencies widespread access to NSA content databases. These same procedures, largely for the same reasons, preclude such access for employees of customer agencies as well. By contrast, broad access to databases that contain exclusively communications metadata may lawfully be provided to other intelligence agencies, because communicants do not enjoy a constitutional expectation of privacy in such information. As a consequence, the Executive Order contemplates its widespread sharing among intelligence agencies.

(U//~~FOUO~~) [redacted] (b)(3)-P.L. 86-36 (b)(5)

1. (U) SIGINT Dissemination Authorities and Limitations

(U//~~FOUO~~) NSA's authority to collect, retain, and disseminate SIGINT is both established and limited by Executive Order 12333, United States Intelligence Activities, and promulgated in various departmental and agency policies.[1] In general, the Executive Order

[1] (U) E.O. 12333 assigns NSA the responsibility for dissemination of SIGINT information. The first Executive Order establishing the intelligence community and authorizing entities within it to conduct particular intelligence activities was an outgrowth of the investigations in the 1970s by committees chaired by Senator Church and Representative Pike. These committees uncovered various abuses by intelligence agencies that concerned the collection, retention and dissemination of information concerning U.S. persons, leading to both the Executive Order

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

requires that all intelligence agencies – including NSA -- comply with Attorney General-approved procedures before disseminating information concerning U.S. persons to other entities. Such procedures, the aim of which is to protect the privacy of U.S. persons, require each agency to make conscious determinations about the information it seeks to disseminate.

(U//~~FOUO~~) At the same time, the Executive Order makes a broad exception to this general rule with respect to dissemination of information within the Intelligence Community (IC). Specifically, it authorizes each agency within the IC – notwithstanding other procedural requirements -- to disseminate information to other appropriate agencies within the IC "for the purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it."

(U//~~FOUO~~) This broad authority to disseminate information to other agencies in the intelligence community without first applying minimization procedures -- itself an exception to the more general restriction on disseminating information concerning U.S. persons -- does not apply to "information derived from signals intelligence."[2] This is so because of the underlying constitutional concerns associated with the acquisition of SIGINT by the government. Specifically, the Supreme Court held 40 years ago that when the government engages in electronic surveillance, it is conducting a search and seizure under the Fourth Amendment; therefore the activity must be carried out in a manner that is reasonable, the touchstone requirement of the Fourth Amendment.

~~(S//SI)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(5)

~~(S//SI)~~ The Courts and Congress have long recognized, in light of the Fourth Amendment, that the appropriate manner in which to address the overbreadth that inheres in the act of conducting electronic surveillance is through the careful application of "minimization

and to the Foreign Intelligence Surveillance Act (FISA), as well as oversight from Congressional committees.

[2] (U//~~FOUO~~) EO 12333, Part 2.3, Collection of Information, states:
Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the Information is relevant to its responsibilities and can be retained by it. [redacted]

(b)(3)-P.L. 86-36
(b)(5)

procedures," procedures designed to reasonably limit the presence of non-pertinent information at each stage of the activity – collection, retention and dissemination. The Attorney General-approved procedures required for every intelligence agency by the Executive Order serve the policy goal of preventing the circulation of information concerning U.S. persons around the government without good reason. The procedures take on additional significance based on constitutional concerns in the case of SIGINT. Compliance with these procedural requirements is what rescues SIGINT activities from potentially plausible charges of unconstitutionality;

[redacted] (b)(5)

~~(S//SI)~~ Constitutionally protected SIGINT information cannot be disseminated, even within the IC, unless NSA first subjects such information to the minimization procedures required by Executive Order 12333. Among the requirements of these procedures are: (1) dissemination of signals intelligence shall be limited to authorized signals intelligence consumers in accordance with requirements and tasking established pursuant to Executive Order 12333, and (2) information that identifies a U.S. person may be disseminated only if one of a group of criteria can be satisfied; these criteria can be generally summarized as a requirement that NSA determine that the identifying information is necessary to understand the foreign intelligence or assess its significance. For the same reasons, entities outside the IC cannot, consistent with the Attorney General-approved minimization procedures, be provided access to databases containing unprocessed and unminimized SIGINT information.

2. (U//~~FOUO~~) Sharing Metadata vs. Sharing Content

~~(S//SI)~~ While the above reflects the current treatment of SIGINT information under the Executive Order and NSA's Attorney General-approved procedures, a significant bright line distinction has evolved in the years since these were drafted. Specifically, NSA employs analysis of what it calls communications "metadata" – information that helps to effectuate communications but is not part of the substantive communication itself -- both as an end in itself and to guide and inform its collection of SIGINT content. While metadata is information derived from SIGINT, and thus is formally subject to the same procedural requirements prior to dissemination as is content, the underlying constitutional concerns that distinguish SIGINT from other intelligence activities do not exist in the metadata context. Indeed, the Supreme Court held in 1979 that a person does not enjoy a constitutional expectation of privacy in the numbers he dials on his telephone, even while he does enjoy such an expectation in the conversation that follows.[4] While statutory protection still exists with respect to communications metadata, we

[3] ~~(TS//SI)~~ [redacted] (b)(5)

[redacted]

[4] ~~(S//SI)~~ The Department of Justice has adopted the position that this analysis extends to other signaling, dialing, routing and addressing information other than the numbers one dials on his telephone, and NSA OGC concurs.

[redacted]

have concluded that greater flexibility exists as a matter of law with respect to the dissemination of communications metadata than exists with respect to dissemination of content.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI)~~ Acting on the distinction between content and metadata and the legal consequences that flow therefrom, NSA has contributed bulk telephony metadata, after masking the numbers that contain U.S. area codes,[5] to the interagency database, where analysts from other intelligence agencies can and do access and analyze it.[6]

(b)(3)-P.L. 86-36

~~(S//SI)~~ In concurring with the dissemination of communications metadata to other IC agencies, OGC relied on two related notions. First, access to this body of metadata as a whole after automatically masking U.S. telephone numbers is consistent with the provision of the Executive Order authorizing each agency to provide acquired information to other appropriate agencies within the IC.

(b)(3)-P.L. 86-36

~~(S//SI)~~ For the reasons set out above, OGC believes that sharing of SIGINT metadata with any U.S. person identifying information removed is permissible currently, with no change to any authorities, and such dissemination is taking place with respect to telephony metadata, and prospects are good for much more robust sharing within the IC in the near future.[7]

0225P (6th Cir. June 18, 2007) at 32 (third party subpoena to service provider to access information that is shared with it *likely* creates no Fourth Amendment problem) (emphasis added).

[5] (U//~~FOUO~~) The legislative history of the FISA makes clear that Congress believed a U.S. telephone number is information that identified a U.S. person.

[6] ~~(S//SI)~~ NSA masks the U.S. telephone numbers for two reasons, one more important than the other: first, NSA does so because it is constrained by its AG-approved procedures to disseminate information that identifies U.S. persons only when it has first concluded that the information is necessary to understand or assess the significance of foreign intelligence. Second, and more significantly, every intelligence agency is prohibited by Executive Order from asking another to do what it cannot lawfully do itself.

[7] ~~(S//SI)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(5)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI)~~ As a practical matter, metadata from electronic communications such as e-mail cannot be similarly shared at the moment under the same theory, because it is not possible to determine what communications are to or from U.S, persons nearly as readily as is the case with telephony, and often is not possible at all.

3. (U//~~FOUO~~) Potential Changes to E.O. 12333 & AG-approved Dissemination Procedures

(U//~~FOUO~~) Finally, as part of the DNI information sharing initiative, the DNI received Presidential approval to recommend revisions to Executive Order 12333. The ODNI OGC is reviewing the document and will provide recommendations to the DNI by October 2007; the NSA OGC is the NSA lead on this action, and is in contact with the ODNI concerning it.

(b)(3)-P.L. 86-36
(b)(5)

(U//~~FOUO~~)

~~(S//SI)~~

~~(S//SI)~~

(b)(3)-P.L. 86-36
(b)(5)

(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(5)

[redacted] (b)(3)-P.L. 86-36 (b)(5)

~~(S//SI)~~ [redacted] (b)(1) (b)(3)-P.L. 86-36 (b)(5)

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[8] (U//~~FOUO~~) In addition to the language of Section 2.3, the Executive Order also states that no Department or agency other than NSA may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense. Section 1.11(b). This provision might also have to be changed in order to effect database access for other agencies.

- [redacted] (b)(1) (b)(3)-P.L. 86-36 (b)(5)
- [redacted]

[redacted] (b)(5)

~~(S//SI)~~ [redacted] (b)(3)-P.L. 86-36 (b)(5)

[redacted]

4. (U//~~FOUO~~) Conclusion

~~(S//SI)~~ There are substantial and well-grounded legal limits on NSA's ability to provide its partners and customers with access to raw SIGINT databases, both those that contain content and those that contain only metadata. Within those limits, NSA has lawfully expanded that access in two ways: with respect to content, we have expanded access by bringing IC partners within the SIGINT production chain in carefully defined circumstances. With respect to metadata, we have aggressively pushed telephony metadata to IC partners, and have plans in place to increase dramatically both the types and the completeness of the metadata we share.

~~(S//SI)~~ Based on the legal and prudential considerations set out above, it seems that access to metadata can and should be widespread within the IC, including military intelligence units, and should be used as a tool to inform and adjust content collection requirements. In the absence of concrete benefit to the intelligence community in meeting the needs of the nation, we think that further requests for broader access to unevaluated and unminimized SIGINT content databases should continue to be on a case-by-case basis, rather than a wholesale basis, and should be the exception rather than the rule. Further, any decision to initiate a change to the NSA's procedures should be considered in light of the benefits weighed against what we think are genuine and serious risks.

(U//~~FOUO~~) Please contact us if you would like to discuss this issue further.

//s//

[redacted] (b)(3)-P.L. 86

Associate General Counsel
(Operations)

July 12, 2007