~~TOP SECRET//COMINT //NOFORN~~

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT

PM 12: 43

U.S. Department of Just[redacted]

National Security Divisi[redacted]

Washington, D.C. 20530

[redacted]

Honorable John D. Bates
Presiding Judge
United States Foreign Intelligence Surveillance Court
Washington, D.C.

Dear Judge Bates:

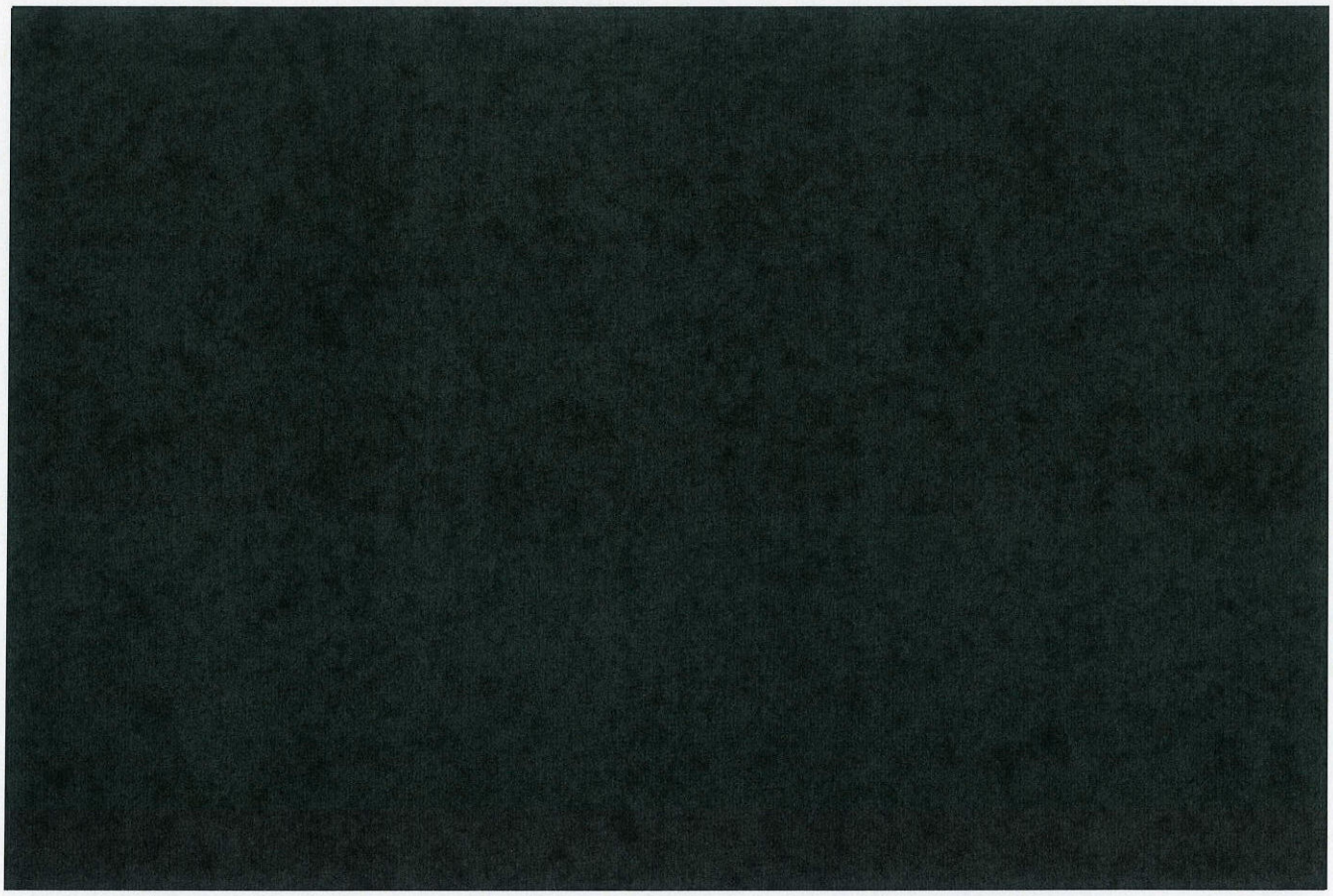
I am pleased to enclose written answers to a number of issues which were raised during our legal discussion concerning bulk collection of metadata through pen register/trap and trace (PR/TT) devices authorized under the Foreign Intelligence Surveillance Act. Should the Court find it helpful, the Government is prepared to discuss our responses with you and your staff at the Court's convenience.

Let me once again thank both you and your staff for your consideration of the Government's proposal to re-initiate the National Security Agency's PR/TT metadata collection and analysis program. Should the Court have any additional questions, comments or concerns, please do not hesitate to contact me.

Sincerely,

David S. Kris
Assistant Attorney General

~~TOP SECRET//COMINT//NOFORN~~



Regarding the Court's request for additional information concerning NSA's ability to track query results and disseminated intelligence reports and recall and destroy the same: ~~(TS)~~

NSA's primary means to disseminate information externally is the formal SIGINT report that carries a serial number for tracking purposes. For a variety of reasons, NSA might find it necessary to revise or recall a serialized SIGINT report containing PR/TT-derived information. The NSA revision/recall process requires the report's originator to issue the recall and nominally consists of both formal and informal processes. Informally, an analyst will typically contact the analyst's Intelligence Community counterparts immediately so that the previously reported information is properly understood and interpreted. In parallel with this informal contact, the analyst also would take prompt action to follow the formal revision and recall procedures. NSA's revision and recall procedures are in compliance with Intelligence Community-wide standards adopted in August 2005 by the Director of National Intelligence. We can provide a copy of those standards upon request. ~~(TS//SI//NF)~~

PR/TT query results are traceable [redacted] NSA uses for PR/TT information. In the event NSA decides to, or is required to purge PR/TT query results [redacted] NSA can do so. However, because analysis is a highly

collaborative human process, PR/TT query results may be shared internally within NSA in many forms, to include information provided orally, in writing, (e.g., email) or in summary form. Therefore, it is impossible to provide absolute assurance that NSA will successfully isolate and delete every shred of internally-shared metadata in every instance. That said, the policies, training, culture, ethos, and professionalism at all levels of the NSA workforce provide a very high level of assurance that such an incident would be remediated with the utmost promptness and thoroughness. In addition, before NSA personnel may disseminate any SIGINT reporting outside NSA, all such reports must be source checked. This should ensure that no PR/TT reports will rely on query results that may have been subject to a purge requirement. This practice also ensures NSA will apply the correct dissemination standard to any PR/TT query results that may contain U.S. person information. ~~(TS//SI//NF)~~

Regarding the Court's questions concerning the application of USSID 18 as a "minimization procedure": ~~(TS)~~

The draft PR/TT application provided to the Court requested that NSA be allowed to apply its standard USSID 18 procedures to the dissemination of PR/TT query results. In light of the Court's concerns with the application of USSID 18 to the dissemination of PR/TT query results, the Government now proposes to substitute a more limited dissemination determination for the determinations set forth in Section 7.2 of USSID 18. Specifically, before NSA disseminates any U.S. person identifying information, an NSA approving official (described further below) will determine, first, that the U.S. person identifying information is related to counterterrorism information (as opposed to the more general foreign intelligence information of USSID 18) and, second, that it is necessary to understand the counterterrorism information or assess its importance (as opposed to USSID 18 requiring either that the information is necessary to understand the foreign intelligence information or assess its importance). Excepted from the determination requirement will be disseminations for purposes of lawful oversight and use or discovery in U.S. criminal proceedings. In the event NSA assesses a need to disseminate U.S. person information that is related to foreign intelligence information under 50 U.S.C. § 1801(e) other than counterterrorism information and is necessary to understand the foreign intelligence information or assess its importance, the Government will seek prior approval from the Court. ~~(TS//SI//NF)~~

In other respects, the Government will apply Section 7 of USSID 18 to the dissemination of query results. In particular, the NSA approving officials who may make the dissemination determination will be the same officials who may make a dissemination determination under Section 7.3(c) of USSID 18. Seven high-ranking NSA officials currently are authorized under USSID 18 to approve disseminations outside NSA: the Director and the Deputy Director of NSA; the Director and the Deputy Director of the SID; the Chief and the Deputy Chief of the ISS office; and the SOO of the National Security Operations Center. The Government proposes that these seven officials approve disseminations of PR/TT query results containing U.S. person identifying information. ~~(TS//SI//NF)~~

Regarding the Court's request for a legal principle that would bound the Government's request for an order permitting access to and use of overcollected data: ~~(TS)~~

In addition to seeking authority to re-initiate collection of new PR/TT information, as described in the draft application presented on [redacted] the Government is seeking an order that (1) authorizes prospective use and disclosure of the data collected under docket number PR/TT [redacted] and previous dockets, and (2) lifts the Supplemental Order issued on [redacted] prohibiting use of the previously acquired PR/TT data.[1] The authority sought with respect to the use and disclosure of the previously collected data is no broader than the authority now sought going forward, and is—in our view—within the scope of the applicable statutes and the Fourth Amendment, but is beyond the scope of the orders entered in PR/TT [redacted] and previous dockets. The Court has expressed concern about issuing an order that authorizes the use and disclosure of data that was in fact collected outside the scope of an existing order but that lawfully *could have been* acquired consistent with the PR/TT statute and the Fourth Amendment. The Court asked whether there was any limiting principle to bound the application of such an order. To illustrate its point, the Court suggested that the Government might seek similar relief if it conducted full-content electronic surveillance without first obtaining a court order under circumstances that would in fact have satisfied the requirements of Title I of FISA. ~~(TS//SI//NF)~~

The Government understands the Court's concern; however, we submit that the extraordinary circumstances under which the Government now seeks the proposed order would provide the Court with ample basis for distinguishing between the relief sought here and the appropriate remedy in future cases. The facts and procedural history of docket number PR/TT [redacted] and previous dockets that authorized the Government to conduct bulk collection of pen register and trap and trace data and to query the resulting data were *sui generis*. Consequently, the relief that the Government seeks here is unlikely to be available in virtually any other case. ~~(TS//SI//NF)~~

[1] [redacted] *See* Memorandum of Law at 78-79. In other matters, the Court has exercised its plenary authority to amend orders that were deficient as a result of the Government's failure to seek authority for activities that were consistent with the governing statute but that were not consistent with the terms of the existing orders. For instance, the Government erroneously filed applications and proposed primary orders and warrants that did not include procedures for the sharing of un-minimized information between the FBI and the CIA or NSA; as such, the primary orders and warrants issued by the Court did not authorize such sharing. Yet, in docket number [redacted] the Court amended prior orders and warrants *nunc pro tunc* to permit interagency sharing of raw FISA information that was already taking place. Similarly, the Government is seeking here to amend the scope of collection that was previously authorized to include additional non-content data that could lawfully have been collected under PR/TT authority. ~~(TS//SI//NF)~~

First, it is extremely unlikely that the Government *could* seek similar relief in any other PR/TT matter. The Court typically lacks jurisdiction over the use and disclosure of information obtained pursuant to a conventional pen register and trap and trace order. Under Section 1842(d)(1), the Court only has jurisdiction to enter orders concerning prospective collection activities and does not possess jurisdiction over the Government's use or disclosure of acquired information (*e.g.*, the querying of resulting data). Thus, the Government would usually have no cause to seek comparable relief in a routine PR/TT case and, even if it did, the Court would lack jurisdiction to furnish it. ~~(TS//SI//NF)~~

Furthermore, the problem of overcollection is unlikely to arise in most PR/TT matters. Unlike typical orders issued under 50 U.S.C. § 1842(d)(1), in docket number PR/TT [redacted] and previous dockets the Government requested and the Court authorized the collection of only specified categories of PR/TT data. While such a limitation on a PR/TT device is within the authority granted by FISA to the Government to apply for and the Court to approve, 50 U.S.C. § 1842(a)(1) and (d)(1), it created a gap that does not usually exist between what an authorized PR/TT device could collect statutorily and what it was permitted to collect. As a result, it created the unusual occurrence of overcollection by a court-authorized PR/TT device, which highlights yet another means of differentiating between the facts here and in other cases. ~~(TS//SI//NF)~~

While the data the Government seeks to access here was collected beyond the scope of the Court's orders, they were nonetheless collected by devices authorized by the Court. Thus, the case at hand is distinguishable from instances in which acquisition occurs without any grant of authority whatsoever, such as in the Court's Title I example. Furthermore, the full-content collection referenced in the Court's example could only result from electronic surveillance, and an order amending a prior order to authorize that collection *nunc pro tunc* would require new findings required by Title I. *See, e.g.*, 50 U.S.C. § 1805(a)(2). In contrast, an order amending PR/TT [redacted] and previous dockets *nunc pro tunc* would not require any new judicial findings to satisfy the PR/TT statute. *See* 50 U.S.C. § 1842(d)(1) & (2). ~~(TS//SI//NF)~~

It is also noteworthy that the data at issue here is non-content information that is not protected by the Fourth Amendment. Accordingly, the Government submits that while it would be appropriate for the Court to permit the requested relief for this class of information in the limited circumstances outlined above, it may not be for constitutionally-protected classes of information in other contexts. It would be particularly appropriate where the overcollection occurred without bad faith or criminal intent under 50 U.S.C. § 1809 and in the context of a highly-technical collection program. ~~(TS//SI//NF)~~

Regarding the Court's request for other instances or case law involving a PR/TT collection that would bear on its consideration of specific aspects of the Government's proposed collection: ~~(TS)~~

Additional/clarifying information regarding what is meant by "application commands" in *In re Application for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass 2005). (U)

The Government contacted the DOJ attorney who handled this case in 2005. He had no further information to provide regarding what the magistrate intended "application commands" to cover since the order that the Government sought under 18 U.S.C. § 3121 in that matter did not request collection of "application commands" or any of the other categories of information that the magistrate's order prohibited the Government from collecting. The Government was only seeking Internet Protocol (IP) address information to determine whether the target was accessing certain Internet gambling sites. Since the magistrate's order clearly permitted collection of the sought after IP address information, the Government did not inquire further into the magistrate's intent or seek to appeal the magistrate's order. (U)

Collection of metadata from inboxes. ~~(TS)~~

NSD has been unable to identify an instance in which the Government sought or obtained an order to collect all metadata for an individual's inbox using either a FISA or a criminal pen register or trap and trace device. Historical electronic communications transactional data are typically obtained using authority other than the PR/TT statute in national security and criminal investigations. ~~(TS//NF)~~

Content, Non-Content, and Dialing, routing, addressing, and signaling information. (U)

There are no cases that address whether electronic communications fall into only two categories (*i.e.*, content and non-content) or whether the PR/TT statutes delineate a third category of communications (*i.e.*, non-content information that is not dialing, routing, addressing, and signaling information). However, the Department has taken the position in congressional testimony that "there is no third category of information that is not comprehended by either 'contents' or 'dialing, routing, addressing, and signaling information.'" Antiterrorism Investigations and the Fourth Amendment after September 11, 2001: Hearing before the Subcomm. on the Constitution of the House Comm. on the Judiciary, 108th Cong., 1st Sess. 12 (2003) at 63-64. As the legislative history for the 2001 amendments to the PR/TT statute indicates, the PR/TT statute was intended to reflect the line drawn by *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979), which distinguished between content information, which was constitutionally protected, and the non-content information, which was not. H.R. Rep. 107-236 at 53. (U)

[redacted]

~~(TS//SI//NF)~~

[redacted]

~~(TS//NF)~~

[redacted]

~~(TS//SI//NF)~~

[redacted]

[redacted]

[redacted] ~~(TS//SI//NF)~~

As argued in the Government's memorandum of law, Congress intended to give the terms dialing, routing, addressing, and signaling broad effect. [redacted]

[redacted] ~~(TS//SI//NF)~~