All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

~~TOP SECRET//SI//ORCON/NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT

- x

IN RE:

[redacted]

Washington, D.C.
October 20, 2015
2:01 p.m.

TRANSCRIPT OF PROCEEDINGS
HELD BEFORE THE HONORABLE THOMAS F. HOGAN
FOREIGN INTELLIGENCE SURVEILLANCE COURT

APPEARANCES:

FOR THE DEPARTMENT OF JUSTICE: [redacted] STUART J. EVANS, ESQ.

FOR THE AMICUS CURIAE: AMY JEFFRESS, ESQ.

COURT STAFF: [redacted]

Court Reporter: [redacted]

Proceedings recorded by mechanical stenography; transcript produced by computer-aided transcription

PROCEEDINGS

THE COURT: All right. Good afternoon. We're here on the matter that we had appointed Amicus counsel to look into under the new statute. I want to introduce you to Judge James Parker Jones from the Western District of Virginia, one of our newer FISA judges, who is just attending this ceremony with me and who will probably be kicking me under the table telling me how to behave here.

This matter before the Court is, as I've said on the report, materials received entitled "The Briefs of Amicus Curiae" from the Amicus we appointed here, Ms. Amy Jeffress, whom the Court acknowledges for her excellent work in a very tight time frame in this matter and appreciates the work that she's given to the Court, and to all of us, for this report.

What I want to start with is a couple of things. One is, I'd like to have introduced the parties who are going to be arguing for the Court for the record. And Ms. Jeffress is one, and we've got about 18 others so I'll assume we'll reduce that to one or two on the government's side, and we won't hear from everybody. But also, after that, anyone who may be intending to be a fact witness, if there's questions I want to ask and develop, if they would introduce themselves, if there's any officials here from the relevant agencies. I think the Court -- counsel for the

Court have at least advised the Court -- the government that my interest, and I believe to -- first of all, my interest really is to the issues she's raised as to the inquiry into the 702 materials by the FBI on evidence of crimes.

The second inquiry that she had -- the first was as to the aspects that we found were appropriate under the new law, I'd call it, The Freedom Act, and some minimization procedures adopted by the CIA, NSA, and then the FBI; and it's the FBI we're concerned mostly about. And the second issue was the retention of materials for litigation purposes, which I think the Amicus has covered as well.

And if the government wants to be heard on any of those others, they can be, but my interest really is in the FBI's minimization procedures and the use of inquiries by the FBI into potential criminal activity in the 702 collections.

So, with that, if we can have the parties who are going to argue introduce themselves first; and then, if there are any identified fact witnesses, we can have them introduced as well.

(b)(6); (b)(7)(C) (b)(6); (b)(7)(C) from the Department of Justice.

MR. EVANS: Stuart Evans, also from the Department of Justice, Your Honor.

THE COURT: All right. And Ms. Jeffress.

MS. JEFFRESS: Your Honor, Amy Jeffress, FISC Amicus.

THE COURT: All right. Thank you.

Any potential fact witnesses you may have here if I have questions to ask, potentially, the FBI?

MR. EVANS: Your Honor, at this time we do have several representatives from the FBI in the room with us. We had not been anticipating, necessarily, presenting a fact witness, but depending on whether the Court had relevant questions, that's something that we can --

THE COURT: If I develop questions that you don't answer and you want to turn to someone else to answer them, then we'll have them sworn at that time. We'll hold off until then.

All right. Well, I think that we will begin with the Amicus and her report, and Ms. Jeffress, you'll want to cover the other areas as well, but I'm obviously interested in what you have developed as an issue in this FBI minimization procedures and their appropriateness or not as it affects the collection and dissemination of matters related to crime and your position in that matter. So if you can take the podium, please.

MS. JEFFRESS: Yes, good afternoon.

THE COURT: Thank you for your work on this matter.

MS. JEFFRESS: Thank you, Your Honor. And thank you for appointing me to serve in this role.

Before I begin, I wanted to add one point to what I set forth in my brief about my understanding of my role as Amicus. One interpretation of the Amicus provision of the statute would be that my job is to present all legal arguments that advance the protection of individual privacy and civil liberties interests.

Many advocacy groups and academic experts presented these arguments to the Privacy and Civil Liberties Oversight Board in much greater detail than I have set forth in my brief. I did not think that the time allowed for my participation permitted me to serve that role, as a privacy and civil liberties advocate, broadly speaking. Rather, my understanding of the role that I was asked to and was able to fill, given the time constraints and my own abilities as advisor to the Court, was really to evaluate the program and to determine whether there were any aspects of the certifications and the procedures submitted to the Court that did not comply with the statutory and constitutional requirements, as I viewed it, with respect to the two specific issues that the Court noted in the order.

So I reviewed the program with that goal in mind and found that I thought that the FBI's minimization procedures are not consistent with the purpose of Section

02:07:24PM 1 702 or the Fourth Amendment because specifically they do not
02:07:27PM 2 provide sufficient safeguards of the U.S. person information
02:07:32PM 3 that is incidentally collected in the 702 -- Section 702
02:07:36PM 4 program.
02:07:38PM 5 To start with, Your Honor, I would first address
02:07:41PM 6 the issue of whether querying warrants a separate Fourth
02:07:46PM 7 Amendment analysis at all.
02:07:47PM 8 THE COURT: Yes, exactly.
02:07:50PM 9 MS. JEFFRESS: You could argue that a query is not
02:07:52PM 10 a search under the Fourth Amendment; that it is --
02:07:55PM 11 THE COURT: Well, if the original materials are
02:07:58PM 12 appropriately collected, which they are, I assume, if they
02:08:03PM 13 permitted them, how is looking at the materials a new
02:08:06PM 14 search?
02:08:06PM 15 MS. JEFFRESS: Right. It's not a new search so
02:08:10PM 16 much as it is a separate action that I think does warrant
02:08:14PM 17 Fourth Amendment scrutiny and needs to be treated as a
02:08:16PM 18 separate action subject to the Fourth Amendment
02:08:19PM 19 reasonableness test, and I think that that is appropriate,
02:08:24PM 20 and I'd also note that the Private and Civil Liberties
02:08:28PM 21 Oversight Board thought so as well. If you look at their
02:08:31PM 22 report on Pages 95 and 96, they talk about how -- and I'll
02:08:39PM 23 just quote -- concerns about post-collection practices such
02:08:42PM 24 as the use of queries to search for the communications of
02:08:46PM 25 specific U.S. persons cannot be dismissed on the basis that

02:08:50PM 1 the communications were, quote, lawfully collected, unquote.
02:08:54PM 2 That's the end of that quote.
02:08:55PM 3 The report, though, goes on to say that the Court
02:08:58PM 4 must consider whether the procedures that govern the
02:09:01PM 5 acquisition, use, dissemination and retention of U.S.
02:09:04PM 6 persons -- and then I'll quote again -- quote, appropriately
02:09:08PM 7 balance the government's valid interests with the privacy of
02:09:11PM 8 U.S. persons, end quote. And I think that that querying
02:09:14PM 9 process, too, is subject to a totality of the circumstances
02:09:18PM 10 test to determine whether it's reasonable under the Fourth
02:09:23PM 11 Amendment.
02:09:23PM 12 THE COURT: Well, if your bottom line conclusion
02:09:27PM 13 is that if the minimization procedures are sufficient and
02:09:33PM 14 consistent with the reasonableness requirement of the Fourth
02:09:36PM 15 Amendment, that wouldn't solve your problem.
02:09:39PM 16 MS. JEFFRESS: That's correct. That's correct.
02:09:40PM 17 And with respect to the NSA's procedures and the
02:09:43PM 18 CIA's procedures, I thought that they did. I thought that
02:09:48PM 19 the requirements that may have been followed before the
02:09:51PM 20 recent changes to the minimization procedures, but that it
02:09:54PM 21 is now very clear, requiring that each U.S. person query be
02:09:59PM 22 supported by a statement of facts that explains why the
02:10:03PM 23 information is being sought and why it's relevant to foreign
02:10:06PM 24 intelligence, or why it's expected to produce foreign
02:10:10PM 25 intelligence information, I thought, justified the query in

a way that the FBI's procedures don't because they allow for really virtually unrestricted querying of the Section 702 data in a way that NSA and CIA have restrained it through their procedures.

I would just also note that the PCLOB report, on Page 96, notes that given the low standards for collection of information under Section 702, quote, The standards for querying the collected data to find the communications of specific U.S. persons may need to be more rigorous than where higher standards are required at the collection stage, unquote. And that's what distinguishes, in my view, Section 702 from the information collected pursuant to traditional FISA applications or in other databases that are collected under more traditional criminal procedure methods.

And then, Your Honor, the government may have arguments on that point that I would want to respond to, but I thought, for the interest of just introducing my position, I would move to the second step in my analysis, which is that the current procedures do not meet the Fourth Amendment reasonableness test, and, as I've already said, I think that the NSA and CIA do have sufficient protections in requiring a written statement that reflects that each specific query is designed to produce foreign intelligence information, and that really justifies the intrusion on U.S. person information that the queries implicate.

The FBI minimization procedures, though, do not. They allow the information to be queried for any legitimate law enforcement purpose, and I find two problems with that. One is that there need be no connection to foreign intelligence or national security, and that is the purpose of the collection, of course, and so they're overstepping, really, the purpose for which the information is collected.

THE COURT: Well, if you look at the -- it is somewhat anomalous, but it is in the statute. I mean, 702, the authorization, the original authorization, it talks about targeting persons reasonably believed to be located outside the United States to acquire foreign intelligence information. That's the purpose of it. But then you go back to the minimization procedures. It's under (h) and, I guess, in 1801(h), "'Minimization procedures', with respect to electronic surveillance, means," and then it talks about (1), specific procedures, which I'm sure you're familiar with, having been at Justice and all, and the Attorney General's adopted these; (2), the procedures that require and what to do about it; and then (3) says, "notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been or is being or is about to be committed and that is to be retained or disseminated for law enforcement purposes."

So the statute recognizes another purpose, does it not, of this collection of the foreign intelligence information as a subsidiary of that or subset that there may be evidence of a crime that's collected as well, which is approved to be distributed under the statute?

MS. JEFFRESS: That's correct, Your Honor, and I would note that you're correct that it also specifies any crime. So it doesn't just restrict that to --

THE COURT: Right, as long as it's a serious crime or a kidnapping or some type that people talk about.

MS. JEFFRESS: No, no, and I think that that is an important point to note. And it explains why the government is permitted to retain and disseminate evidence of a crime, and that's that, you know, when the government collects it pursuant to these lawful authorities, if there is evidence of a crime, it would be somewhat counterintuitive for the government not to be able to use that and to act on it.

But I think that the use -- the querying process is different because there is no finding that this incidental collection is such evidence, and that takes me to the second point that I wanted to make about the FBI's minimization procedures, which is that there are -- there is no limitation on what type of matter can be the subject of a query. So an assessment can be the subject of a query, and assessments can be initiated for virtually any reason. I'm

sure there are limits on improper reasons, you know, racial discrimination and things like that, and that's out of bounds, of course, but really there is no threshold that needs to be met.

And for an assessment, I would note that there are restrictions even on the use of grand jury subpoenas for assessments. So grand jury subpoenas can only be issued to request subscriber information for telephone numbers or email addresses, and so they're really viewed as considered the very lowest of the purpose for which you would need a query.

And I think that that opens up the Section 702 database to a really very wide-ranging, really virtually unrestricted use by the FBI that I think should be cabined in order to meet the Fourth Amendment reasonableness test.

I found that that unrestricted querying just is inconsistent with the language and the analysis in the FISA Court of Reviews case *In Re: Sealed Case*, which stated plainly that the FISA process cannot be used as a device to investigate wholly unrelated crimes, and I think that that's what this querying process allows the FBI to do without any restriction of the querying process.

THE COURT: That's Judge Silberman, 736 of his opinion, you're talking about. He says, for example, a group of international terrorists engaged in bank

robberies -- which is something I'm going to raise in a minute -- in order to finance or manufacture a bomb, the evidence of bank robbery should be treated just as evidence of a terrorist act itself, but the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

MS. JEFFRESS: That's what I thought was the language that made me -- gave me pause about what the FBI is doing with the Section 702 database here because that's exactly what it seems these minimization procedures permit.

THE COURT: That case, in essence, approved the practice of retaining and disseminating information about possible crimes --

MS. JEFFRESS: It does.

THE COURT: -- under proper controls.

MS. JEFFRESS: Right. And there's a very careful balancing in the opinion of the purpose -- the national -- the foreign intelligence purpose of the statute and the need to preserve and use evidence in a crime, but I thought it was a very careful analysis.

And on Page 735, there's also some language that I thought was instructive where the Court wrote, "The addition of the word 'significant' to [the section at issue] imposed a requirement that the government have a measurable foreign intelligence purpose other than just criminal

prosecution of even foreign intelligence crimes." So the Court was grappling with what purpose the statute required, and I think came to a conclusion that's instructive in this context.

The last point that I would make, Your Honor, and then I'm happy to answer specific questions from the Court, but I thought that the government actually appeared to recognize the need for limits in one regard with respect to the changes that have been made to the NSA and CIA minimization procedures, but also even in the government's brief on Page 14, the government says, "Given that FBI is a law enforcement agency as well as a member of the intelligence community, the ability to query for evidence of a crime using U.S. person identifiers can help the FBI pursue important leads regarding criminal activity."

And I think that's good language, "important leads." They clearly want to be able to use it for examples that they cited: espionage, cyber crimes, terrorism, and, you know, they said perhaps to help locate a kidnapper. And I think that that -- that may be justifiable, but there's no restriction in the minimization procedures that restrict it even to important leads or important crimes. They can use it for any purpose, and I just found that to be beyond --

THE COURT: Is it your impression, from what you've been able to read in the PCLOB report, that an agent

or analyst who is conducting the assessment of a nonsecurity crime would get generally responsive results against the queries in the 702-acquired data, and I'm referring, not to mislead you, that the PCLOB reports says, and notably, the FBI says they don't get that.

MS. JEFFRESS: I saw that, and I don't know what to make of it because it's anecdotal, and they didn't have much support for it, but I take it that that is true, and maybe you can find out more. But I don't know that that is -- that that answers the question because going forward it may be that it does draw responsive data or it may prove the point, Your Honor, that maybe they don't need to be querying the Section 702 database in cases that are not national-security related.

THE COURT: All right. If the relevant minimization procedures were modified, as you suggested to us in the beginning, assuming incorporating executive branch policies that limit this to national security, provided these inquiries are serious crimes and that -- and to be used as evidence in serious criminal cases, I mean, would the modification be sufficient to satisfy, you think, the concerns you have about violating the Fourth Amendment?

MS. JEFFRESS: Your Honor, I didn't make a specific recommendation for what -- how the FBI should meet this.

02:21:00PM THE COURT: Did you talk about maybe they should record or have a written inquiry each time they want to do this? Every officer in the FBI would have to sit and write a justification up when he wants to send an inquiry in.

02:21:13PM MS. JEFFRESS: That is one option, Your Honor, and the option that you just mentioned a moment ago in terms of limiting the types of matters that can be the subject of a query would be another; or perhaps you'd have both, given the sensitivity of the incidentally collected information.

02:21:30PM But I would note that the FBI's general counsel, James Baker, testified three times that I'm aware of, possibly more than that, before the Privacy and Civil Liberties Oversight Board. He's one of the most authoritative experts on the program, and I think that he would certainly be highly capable of designing minimization procedures that would provide appropriate restrictions but also allow the FBI to use the information for purposes that are really justified and necessary to protect national security.

02:22:04PM But I would note both of those options are ones that I think probably would satisfy the Fourth Amendment reasonableness test but are not present in the current procedures.

02:22:16PM THE COURT: One of the things that was pointed out in PCLOB, and some of the government's materials as well, is

that this set of data is commingled with other data the FBI has normally in their files and that it's essentially a practical impossibility to distinguish between the two. Would your requirement sort of be putting more emphasis on the minimization procedures or making them more restrictive and require them somehow to separate those out?

The government can answer in a minute as to that. But would that be necessary, you think, to have a separate data bank?

MS. JEFFRESS: That, again, is why I didn't delve into the specifics of what I think would be required. I think separating it, if that's not possible, then perhaps they need a justification and a set of requirements surrounding the use of the querying in the entire database, and that may be more practical.

THE COURT: I'll ask the government. I think it's flagged somehow that it's NSA material anyway within the same data bank. It is flagged because they do have some procedures about that.

All right. Let me just switch with you for a minute. On the retention -- the second prong of your assignment that you've accepted from us was a retention for litigation purposes beyond the normal purging time frames. Even though there's an exception to the minimization procedures that we've adapted and that are normally

required, you had felt that that was a justifiable exception?

MS. JEFFRESS: I did, Your Honor. I just couldn't see how the government would handle those competing directives other than they have. It seems to me that the government's made a real effort to comply with the destruction requirements, but in the face of court orders, where information is specifically designated as being necessary for specific cases, I think that those specific cases are good cause to maintain the information despite the otherwise applicable destruction requirements.

So especially after having read the reports that the government files annually with the Court, which your order from 2014 required them to file, I thought that the material that was being preserved was limited in nature. It was specifically preserved for purposes of, you know, a relatively small number of cases, and I just don't know how else the government would accommodate the needs in those cases, which seemed to me to be wholly legitimate and specific. Where, of course, the destruction policies in the minimization requirements are important, and they're important in the Court's analysis of the program overall, they're also general in nature in that they're, you know, age-off requirements that apply to the entire body of data and not to specific elements of it apart from that material

that is required to be destroyed because it's inadvertently collected and really shouldn't have been collected, but collected basically because of errors.

So I thought that the government had handled that appropriately, Your Honor, and, with the Court's oversight, I don't have any concerns about that aspect of the procedures.

THE COURT: All right. Anything else you want to address the Court about on these issues at this time?

MS. JEFFRESS: No. Do I come back or...?

THE COURT: You'll get a chance to come back.

MS. JEFFRESS: Thank you, Your Honor.

THE COURT: Thank you, Ms. Jeffress.

(b)(6); (b)(7)(C) I'll hear from you at this time on behalf of the government. And you can focus, I think, your argument principally on the issues we've discussed with Ms. Jeffress and explain why this querying of the U.S. person information should be subject to Fourth Amendment search review or what is reasonable looking at this that can be done with proper minimization procedures to make sure that this is being appropriately done under the law.

(b)(6); (b)(7)(C) Thank you, Your Honor. And the government appreciates your careful consideration of these issues. We appreciate the views of Amicus and the ability to address them in this hearing.

02:26:59PM To begin with, to start with the Fourth Amendment issue that you addressed, we would agree with your earlier comments that the querying of this information after it's been lawfully acquired is not a separate Fourth Amendment event. It is not a separate search, and Amicus did not cite case law that suggests that it would be. It's certainly the case that the program as a whole must comply with the Fourth Amendment and must be reasonable under the Fourth Amendment.

02:27:28PM THE COURT: Well, let me ask you about that. Suppose a local agent in the field office runs across somebody's name and, without any basis to think that he did anything wrong, he starts making an inquiry into the database of the FBI and gets a hit that there are some 702 evidence or materials that he can't see so he asks someone who has a FISA clearance to go ahead and make the inquiry, and they bring back something like a credit card fraud or something, and that has nothing to do, that he can tell, with any foreign intelligence issues. I mean, aren't there some protections that should apply there?

02:28:20PM (b)(6); (b)(7)(C) So I want to be very clear on that point. The FBI can only conduct a query for an authorized purpose. Now, that authorized purpose for FBI is different than NSA and CIA, but it must be an authorized purpose. They cannot go in and query because they come across someone who, as you point out, hasn't done anything wrong. That is

already prohibited by the minimization procedures.

The authorized purpose that the FBI had is either for queries that are reasonably designed to return foreign intelligence information or reasonably designed to return evidence of a crime. Those two purposes, as Your Honor points out, come directly from the definition of minimization procedures in the statute.

They are also the joint purposes of the FBI itself. It is a dual law enforcement and intelligence agency, and certainly one of the things that we've learned in the last 15 years is that we can't make artificial distinctions between these two roles of law enforcement and intelligence, and so perhaps hypothetical examples do help.

You can have instances, for example, where the FBI is investigating a crime. Let's take a minor crime as opposed to the more major ones. Let's take a minor crime like something like cigarette smuggling, a federal offense, or money laundering. The FBI queries in these federated systems. They query not just the 702 information but other information that they obtain from intelligence and law enforcement, from their foreign partners. Query across.

When they conduct that query, they're not looking at that time for foreign intelligence information. They're looking for evidence of that crime, but to the degree something then pings in the 702 and connects a dot that they

didn't know was there -- so they find, yes, my cigarette-smuggler actually is speaking with [redacted] individuals -- that investigation has now taken a very different turn. Now we have a national security element to that investigation.

But when that query was conducted, the government didn't know that. We can only connect the dots by looking at the information. When we ran that query, we were doing so because we were looking for evidence of a crime across all of our systems.

Those federated queries are something that come from a number of experiences the government's had and a number of the commission reports. So going back to the 9/11 Commission, that Commission was quite critical of the government saying that one of the weaknesses that enabled the 9/11 attacks to occur was the government's failure to make use of information already in its repositories. There were three hijackers, the Commission found, that we couldn't identify and didn't because we didn't look at all the information that we already had.

To use an example more recent and even more on point, the Webster Commission's report on the Fort Hood attack criticized the government's queries of information in its possession. The people doing the assessment of Nidal Hasan did not identify several messages between Anwar Aulaqi

and Nidal Hasan, and the commission deemed it essential that the FBI possess the ability to search all of its repositories and to do so without balkanizing those data sources.

And so these systems that do these federated queries that allow us to, yes, to query the 702 information, but all of these sources are in direct response to those findings, and they're in direct response to our efforts over the last 15 years to bring down this artificial wall between the law enforcement mission of the FBI and its national security intelligence mission.

THE COURT: As I asked the Amicus, the PCLOB said that anecdotally the FBI has advised the board that it is extremely unlikely an agent or analyst who is conducting an assessment of a non-national security crime will get a response or result from the query against 702-acquired data, and I know Rachel Brand and her counterparts say it never happens, according to her.

Do you know anything about that?

(b)(6); (b)(7)(C) So we would say at the very least it would be extremely rare, and we believe that's one of the many reasons why the privacy impact of these queries would be quite low.

It's not surprising that it would be quite rare. We are talking about a targeted program. Targets for 702

collection have to be non-U.S. persons outside the United States who the government reasonably believes possess or can communicate foreign intelligence information. It's a big program, but as the Court recognizes, it's a targeted program. This is not bulk surveillance.

I know in the Amicus brief there's a footnote about the government conducting surveillance of entire geographic regions. That is not this program. This program is targeted on people outside of the United States, and the likelihood that in any given query information about a U.S. person is going to be returned is quite low. However, if it happens, when it happens, it can be quite significant. It can connect that dot that we were not aware of before.

THE COURT: Is there any requirement in the minimization procedures that's been suggested by the government now that the FBI personnel be required to record the purpose of the query? Is there a written statement made or anything?

(b)(6); (b)(7)(C) So that is something that the government has taken a look at in the past. We believe that the procedures, as they are, are sufficient, both as a statutory and constitutional matter. We don't believe that a difference in documentation -- and let's be clear, what we're talking about is a difference in documentation. FBI does have to document some aspects of their query, as do NSA

and CIA. The particulars of that documentation vary, but there is a documentation of parts of it throughout, and I can explain that in more detail.

THE COURT: What's the rationale for the difference in the CIA/NSA minimization procedures and the FBI minimization procedures?

(b)(6); (b)(7)(C) So it goes fundamentally to the different missions of those organizations. The NSA and the CIA have a -- are foreign-focused intelligence organizations. They have little need usually to query U.S. persons. It happens much more rarely, and they don't have that law enforcement mission that the FBI has.

FBI has all of those things. FBI had also -- as I mentioned in the commission report, has a duty to do these federated queries across these systems, so they're conducting queries on a much more regular basis. But the fact that there isn't a documentation requirement with respect to the justification doesn't mean that the queries don't have to be documented.

So what is required of the FBI is that every query is recorded. Those query terms are recorded; what the agent -- which agent did the query is recorded; whether the information has been exported to another system is recorded.

And what the National Security does with those records for the FBI is we go out to about 30 field offices a

year, and we sit down with the agents and analysts, and we make them justify the queries; take a sample, and make them justify those queries. And what we've found is that they can. The agents and the analysts, they understand the rules because they have to have a justification. They can't, to use your first example, query someone just because they come across them, and they've done nothing wrong. They know they have to have a justification, and they've given them to us.

We've done some effective oversight of that. We've found no systemic problems. We've found FBI agents and analysts understand the rules. We've found a few isolated incidents, but those incidents have been things like an individual querying their own name for work flow purposes.

THE COURT: In your example you gave, for instance, of cigarette-smuggling which turns out to be potentially related to national security matters, is the experience such now you think the FBI queries of 702 data can be limited to national-security-related crimes? I mean, do you have a database where you can recognize crimes generally associated with national security?

(b)(6); (b)(7)(C) I think limiting the queries to national security crimes is going to cause us to miss connecting some of the dots or something we do not realize is a national security event before we conduct the query

and, in fact, has national security implications.

So to take another example, for example, for cyber security. FBI could be investigating a spear phishing attempt, a criminal attempt to access a computer. They have no indication that there's any sort of foreign connection. They run a query like this in those federated systems, and they find out -- they did not know before, but they find out that, you know, we have [redacted] cyber hackers who have been using this account. They just didn't know that.

So if we limit what those queries can have, we're going to miss those instances where we're going to make that connection. As I said, those connections are going to be rare, but very important when we find them.

THE COURT: Again, on the numbers, is there any FBI information available as to the actual numbers of queries that come up with hits that 702 evidence is available about a crime? And maybe it happens a hundred times a month, or is it once a year? I don't know.

[redacted] So we don't have -- we, unfortunately, do not have specific information about when evidence of a crime is returned from one of those queries. What I can say, Your Honor, is that in no instance to date has the government used, in a criminal trial or in a non-national security matter, 702-obtained information.

02:37:44PM THE COURT: So I understand the program -- I want to make sure I understand it. The 702 data that is mixed in with the other information you have is still segregated in a sense that when a query is made it hits a 702 data. That comes back that way. I mean --

02:38:03PM (b)(6); (b)(7)(C) Certainly, Your Honor. It's identified as FISA information, and this can occur in one of two different ways in this federated system.

If the agent has a subject matter reason to have access to FISA information and has the full training in the FISA minimization procedures, when they run a query like this, they will return the results, and it will be clear to them that this is FISA information and, in fact, as they look at it, 702 information.

If the agent does not -- is a criminal agent working mostly those cigarette cases, they would not have access to FISA information in the course of their normal duties. They would not have the FISA training. When they run that same query, they would -- the content would not be returned to them. Metadata would not be returned to them. The only thing that would be returned to them was an indication that there is some information available in this database that contains FISA.

And what the procedures before you do is they require that individual to go to someone who does have the

training and the minimization procedures. They have access to the data to rerun the query. And there is a new requirement, a new restriction, that has not been in the procedures before that also requires supervisory approval both from the criminal agent's supervisor and the national security agent's supervisor before that second query is run to ensure that it's appropriate, to ensure -- to use your first example again -- they are not running queries for someone for whom they have no reason to.

THE COURT: Again about whether you can ask questions whether they be related to national- or foreign-intelligence-related crimes was Judge Silberman's expression that the Amicus pointed out where he talks about international terrorists engaged in bank robbery that's obviously to finance or manufacture a bomb. The evidence of bank robbery is treated just like a terrorist act itself. I'm not going to get into that.

So he concludes, then, but the FISA process cannot be used as a device to investigate wholly unrelated ordinary crime.

(b)(6); (b)(7)(C): So I think unfortunately the quote the Amicus identified really turns the actual holding of *In Re: Sealed Case* on its head. So *In Re: Sealed Case* was a case about the initial targeting of an individual, getting that authorization from the FISA court in order to -- and it

was saying that we could not get a FISA for purely criminal reasons. But the holding of that case was that not even constitutionally a primary purpose of the government, but only a significant purpose of the government needed to be to obtain foreign intelligence information.

And Amicus's brief repeatedly refers to the purpose, the purpose. The purpose is an even stronger standard than a primary purpose, which has been rejected by *In Re: Sealed Case* and has been rejected by Congress in the Patriot Act. It must be that it's a significant purpose, and in 702 we have that purpose because when we're acquiring the information, we are acquiring information only because we've assessed that the target of that collection, in addition to being a non-U.S. person who we believe to be outside the United States, either possesses or is communicating foreign intelligence information.

THE COURT: PCLOB says at one point -- and really I'd like the opportunity to question what the PCLOB has said. But the PCLOB said at one point, at Page 161 there's a statement -- I made a note -- that it received -- the FBI receives only, quote, a small portion of the 702 collection.

Do you know what that is, or --

(b)(6); (b)(7)(C) Yes, I do, Your Honor. Thank you. That's actually a point I was hoping to return to.

(b)(1); (b)(3); (b)(7)(E) [redacted]

(b)(1); (b)(3); (b)(7)(E)

[redacted]

Not surprisingly, the individuals that the FBI is identifying are related to the things that FBI investigates. They are the CT cases. They are the cyber cases, weapons of mass destruction. Those are cases that they have already opened.

THE COURT: But when an FBI analyst has supposedly been tasked to email accounts, and he's reviewing all the emails, and he has a task because you were talking about weapons of mass destruction or something, but in there he finds ordinary credit card fraud, would that change the analysis of whether he could then use that and proceed with an investigation? It wasn't what he was looking for. Do you know anything about that?

(b)(6); (b)(7)(C) It was not originally what they were

looking for, but FISA -- and this is not just the 702 -- FISA from the beginning, from 1978, has recognized that the FBI might come across evidence of a crime in the course of doing their investigation.

Now, I would say, as I said earlier, the government has not used 702-obtained information in a non-national security crime to date. This is an instance where, and sort of interestingly, the interest of defendants and the interest of the intelligence community happen to align, right?

The intelligence community -- this is -- puts a great deal of importance on this program. They're not going to risk their sources and methods for this important program on an ordinary crime, and that's where the use policy that the government announced earlier this year stems from, is the fact that the information is not going to be used in an ordinary crime because we're not just going to risk our sources and methods in those instances.

THE COURT: Is there any reason why the minimization procedures could not incorporate some restrictions to limit the searches to, as I said, certain crimes related to national security?

I'm not sure where -- the Amicus has argued in her brief, and she can raise this again, but that it's -- there are certainly possibilities, if not probabilities, that

there will be incidental collection. I mean, we're talking [redacted] of bits of information, collection of American conversations or whatever with others abroad, et cetera, or emails, et cetera, that are totally innocent, and it seems to me that the minimization procedures in effect now would allow the FBI to make inquiries that would then go into this information to see what might be there that would return anything about a crime because they had some -- you're saying some investigation open about somebody. But I don't know how you limit that appropriately to satisfy the requirements in the statute. There has to be reasonableness under the Constitution for this search or this inquiry, at least, to be made of this information. I'm struggling with that a little bit.

(b)(6); (b)(7)(C) : I think, from a statutory perspective, as you mentioned earlier, the statute doesn't distinguish between crimes. It just says evidence of a crime.

With respect to reasonableness, the government would really assert that when the Court looks at these procedures, they need to look at the sum of these procedures as opposed to isolating aspects of them. It starts with a targeting and a limited collection aperture of the targeting in the first place and for those purposes. That doesn't mean we will not receive some incidental U.S. person

information. That's probably only where it starts.

You also have the access controls that are limiting this information to individuals who are working on these national security issues. You have the controls on retention, you know, the controls on dissemination. You have the controls of attorney-client communications. You have the controls on querying that can only be done for an authorized purpose.

All of these privacy controls are an integrated approach to protect Americans' civil liberties and privacy, and that whole of all of those protections, we have found, does a very good job of ensuring that no one is rifling through these communications.

THE COURT: Do we have numbers or ballpark figures as to the number of inquiries made by the FBI? Not just for crime, but just the numbers made to the 702 collection of materials on a yearly basis?

(b)(6); (b)(7)(C) So we don't have specific numbers. It's a substantial number of queries, particularly because of these federated systems. They don't break down by U.S. person or non-U.S. person. A query is a query. But it is a routine and encouraged practice for the FBI to conduct queries at the beginning of an assessment.

This is the way that the FBI, looking at its lawfully acquired information, makes its initial

02:47:46PM determinations about whether further investigation, which
02:47:50PM often involves further more privacy invasive steps, is
02:47:52PM warranted or not. They conduct these queries, and then,
02:47:56PM based on the results, either have confidence, no, there's
02:47:59PM nothing here, and stop, or there is some additional
02:48:02PM information that we need to investigate.
02:48:05PM THE COURT: What problems would arise if the
02:48:10PM Amicus's suggestion of modifying the minimization procedures
02:48:15PM to be more precise and tightly controlled, although it may
02:48:21PM be a written authorization, et cetera, would arise to the
02:48:25PM FBI by having to do that?
02:48:27PM (b)(6); (b)(7)(C) So maybe to start with that written
02:48:28PM justification requirement. Because these systems are
02:48:33PM queried on such a routine basis, these federated systems in
02:48:37PM some ways are FBI's Google of its lawfully acquired
02:48:42PM information. They are quite routine. They must have that
02:48:46PM justification before they query, but they're quite routine
02:48:50PM queries.
02:48:50PM And so the implications here -- there are
02:48:54PM technical issues we would have to work out. But far more
02:49:10PM concerning to us than the technical issues are the practical
02:49:12PM ones. If we require our agents to write a full
02:49:16PM justification every time -- think about if you wrote a full
02:49:19PM justification every time you used Google. Among other
02:49:22PM things, you would use Google a lot less. Well, one of the

things that we learned from these commission reports is that's not what we want. We want the FBI to look and connect the dots in its lawfully acquired information.

So there's a practical limitation that's going to just cause the FBI to use these tools that we've spent a good deal of time and learned some very hard lessons in order to have to build; and in addition to that -- I'm sorry, I'm losing my place here for a moment. In addition to that, once you have that requirement, that bureaucratic requirement, the FBI really has two choices. Either you're going to have agents use the system less, or alternatively -- and the FBI, when it was examining this very kind of requirement said, well, one of the things we might have to do is then pull the 702 information out. Pull it out of the federated system. Balkanize the data again.

THE COURT: That was my next question.

(b)(6); (b)(7)(C) Unlearn that lesson and have it in a separate repository. And if we have it in that separate repository, again, we're going to miss our dots because we now have to query multiple systems. It's that querying of multiple systems that has gotten us, as the government, again and again and again. We finally, I think, have learned our lesson. We don't want to unlearn it.

THE COURT: All right. Do you have any other issues you wanted to address in this matter?

02:50:44PM [(b)(6); (b)(7)(C)] Your Honor, if you have no further questions.

THE COURT: Anything else?

All right. Thank you, [(b)(6); (b)(7)(C)] I appreciate it.

[(b)(6); (b)(7)(C)] Thank you, Your Honor.

THE COURT: We'll get Ms. Jeffress up and get a chance for her last word here.

MS. JEFFRESS: Thank you, Your Honor. I'd like to first go back to the question that the Court asked [(b)(6); (b)(7)(C)]

THE COURT: Can you lower the mic a second. I can't see. That's why.

MS. JEFFRESS: There you go. Better?

THE COURT: Thank you.

MS. JEFFRESS: I wanted to go back to the question the Court asked with respect to the rationale for the difference between FBI's procedures and NSA's and CIA's, and that's, in fact, the subject that [(b)(6); (b)(7)(C)] was just talking about, that it would be more difficult to adopt those -- to adopt similar procedures because the FBI's queries are so frequent. I don't think that that is necessarily an answer that justifies not complying with the Fourth Amendment. It doesn't seem to me to be too unreasonable to require.

As (b)(6); (b)(7)(C) explained, the queries are already recorded, and when the Department of Justice goes to field offices to do oversight, they require the agents to explain them, and they have, in fact, found, which is good to know, that the agents can explain them. I don't think it's a real imposition to have the agents have to put that explanation in writing before they conduct the query, and I think it is a step that perhaps may mean that they don't always do it in the cases where now they do always do it, but perhaps that means because now they are doing it in cases where there really isn't a real obvious need to be doing it, assessments that aren't sufficiently important, and other circumstances.

So I don't think it's an unreasonable requirement, and I don't think that it would rebuild the wall or render the government unable to connect the dots. If the matter is important enough where the dots are important and could be connected, I think that the FBI will do it.

I also wanted to explain the point that I made about the scope of the incidental collection. I did not mean, in my Footnote 7, to endorse what the ACLU statement said about the program, and I actually don't think that statement is accurate. What I was really trying to do is to say, "Here's the extreme end of this criticism."

But I do stand by the text that I wrote with respect to how often Americans' communications could be

02:53:19PM 1 intercepted incidentally because the targets are so wide,
02:53:24PM 2 and (b)(6); (b)(7)(C) actually did explain that to some extent;
02:53:27PM 3 that the FBI only receives a certain portion of the Section
02:53:31PM 4 702 information, which is helpful. But the entire body of
02:53:34PM 5 it really does likely intercept lots of information of, you
02:53:41PM 6 know, Americans who are communicating with friends overseas
02:53:43PM 7 who, as I pointed out, [redacted]
02:53:48PM 8 [redacted]
02:53:50PM 9 So I thought that the scope was really very --
02:53:53PM 10 potentially very broad, although I didn't take the same view
02:53:56PM 11 that the ACLU took of that.
02:53:58PM 12 And, Your Honor, you mentioned that your concern
02:54:01PM 13 is with, you know, obtaining information about credit card
02:54:04PM 14 fraud and the like, and I think that they're -- that's one
02:54:07PM 15 issue, but there is a potentially greater issue with just
02:54:10PM 16 the intrusiveness of having the innocent communications
02:54:14PM 17 reviewed. And there are lots of private communications that
02:54:16PM 18 take place over email that people who are -- whose
02:54:20PM 19 communications are incidentally collected would not want to
02:54:22PM 20 be reviewed for any purpose, and so I think there should be
02:54:26PM 21 stricter limitations for that reason.
02:54:28PM 22 I wanted to also respond to the comment about my
02:54:33PM 23 turning the logic of *In Re: Sealed Case* on its head. And I
02:54:39PM 24 understand [redacted] (b)(6); (b)(7)(C) point, but I don't think that I did
02:54:42PM 25 that because the analysis in that case was really whether --

it was balancing the prosecution being -- prosecution of national security crimes for the most part being a purpose of the collection versus just a collection of foreign intelligence information. So it really didn't go into the sort of issues surrounding the prosecution of unrelated crimes, which is my central concern here.

And I think -- let me just check my notes for one thing, Your Honor.

Finally, I think that the query, as (b)(6); (b)(7)(C) pointed out, if it is reasonably designed to return foreign intelligence information or evidence of a crime, that can be explained in a statement that is a relatively minimal imposition on the FBI.

I would just conclude by saying that I don't think that the FBI will voluntarily set limits on its querying procedures because law enforcement agencies tend not to take steps to restrict or limit what they can do, for obvious reasons, and that's, you know, giving them the full benefit that they're very-well-intentioned and they want to do their job as best they possibly can. But the incentive is that if you give them a program or a database or any other power, they will use it to the fullest possible extent, and I think that in this case the procedures could be tighter and more restrictive, and should be, in order to comply with the Fourth Amendment.

02:56:18PM THE COURT: Thank you very much, Ms. Jeffress.

02:56:21PM I'm going to see if counsel for the Court has any particular question they wanted to raise.

02:56:25PM (b)(6) Your Honor, can I ask one question?

02:56:29PM (b)(6); (b)(7)(C) can I --

02:56:32PM THE COURT: You can sit down.

02:56:34PM (b)(6) -- ask you one follow-up question on something?

02:56:35PM So just following up on the statement that the judge mentioned, the anecdotal statement, and this other statement in the PCLOB report, I think it's in the separate Brand and Cook part of the report: "We are unaware of any instance," this says, "in which a database query in an investigation of a nonforeign intelligence crime resulted in a hit on Section 702 information and much less a situation in which such information was used to further such an investigation of prosecution."

02:56:41PM

02:56:43PM

02:56:47PM

02:56:53PM

02:56:56PM

02:56:59PM

02:57:03PM

02:57:07PM

02:57:10PM

02:57:12PM I think you made the point, you know, that that undercuts the notion of this being overly intrusive, but at the same time doesn't it undermine the -- I mean, how do you reconcile that with the national security purpose of the collection as a whole?

02:57:14PM

02:57:19PM

02:57:23PM

02:57:26PM

02:57:28PM You gave a bank robbery example, or I think it was -- I can't remember exactly what it was, but --

02:57:31PM

02:57:34PM THE COURT: Cigarettes.

02:57:35PM 1 (b)(6) Cigarette smugglers. Are there any
02:57:38PM 2 examples where queries unrelated to foreign intelligence on
02:57:43PM 3 the front end resulted in the acquisition of information
02:57:49PM 4 relating to foreign intelligence? And if the answer is no,
02:57:52PM 5 then how does this process really serve the overall national
02:57:57PM 6 security purpose of Section 702?
02:58:00PM 7 (b)(6); (b)(7)(C) So to answer your question, I don't
02:58:03PM 8 have a smoking gun example for you, and I think that's for a
02:58:07PM 9 couple of reasons. One is because, again, the collection
02:58:10PM 10 that is being acquired is of the non-U.S. persons outside
02:58:13PM 11 the United States. We would expect queries -- particularly
02:58:16PM 12 queries not for foreign intelligence information, but
02:58:19PM 13 instead for evidence of crime -- to very rarely respond to
02:58:22PM 14 anything.
02:58:22PM 15 And for a second reason, which is it is --
02:58:26PM 16 querying is one tool in FBI's toolbox, and to discern that
02:58:31PM 17 any individual query was the thing that broke open the case
02:58:34PM 18 is often a very difficult thing to do.
02:58:37PM 19 That said, what we have found, again, just
02:58:43PM 20 returning to those -- returning to the commission reports of
02:58:50PM 21 the past, is that we do not want to limit our ability to
02:58:53PM 22 connect the dots. We don't know beforehand, before we do
02:58:57PM 23 the query, whether the information is going to be responsive
02:59:00PM 24 and is going to lead to that national security angle.
02:59:05PM 25 And we have appropriate controls. We limit the

02:59:08PM 1 access. We limit the retention. We can limit the
02:59:10PM 2 dissemination, and we have our policy on use. We have a
02:59:14PM 3 variety of limitations designed, particularly designed to
02:59:18PM 4 protect the privacy and civil liberties of individuals, but
02:59:22PM 5 what we don't want to do is to balkanize our data to then
02:59:28PM 6 limit our ability to find that dot that is out there in the
02:59:31PM 7 case where it is, in fact, important. It is -- and I think
02:59:34PM 8 this is something that we also saw in the PCLOB report.
02:59:38PM 9 It wasn't that the PCLOB report thought there were
02:59:40PM 10 no concerns. Where they ultimately came out on this was
02:59:43PM 11 where are the proper places to put those protections, and we
02:59:46PM 12 believe the proper places are to limit those queries to
02:59:50PM 13 foreign intelligence information or evidence of a crime, to
02:59:53PM 14 limit that access, to limit the targeting to foreign
02:59:56PM 15 intelligence information, to limit the retention and
02:59:59PM 16 dissemination, to limit their use.
03:00:02PM 17 We've imposed all of those, but what we don't
03:00:06PM 18 believe we should do is limit our ability to find the dots
03:00:08PM 19 where we weren't expecting to find them.
03:00:13PM 20 (b)(6) Thank you, Your Honor.
03:00:18PM 21 (b)(6) I guess what I want to ask about is
03:00:21PM 22 federated queries, which it sounds like is the principal
03:00:25PM 23 means by which FBI personnel queried the 702 data. Is that
03:00:31PM 24 correct?
03:00:31PM 25 (b)(6); (b)(7)(C) It is one of the means. So the FBI

has both a repository of information that includes FISA and some other information, for example, like national security letter information that it queries, but it also has the system -- I believe it's DIVS -- that allows these federated queries of not just the FISA information but, for example, CBP records, foreign intelligence reports, FBI's own case files. It is really those federated queries where those come into play.

(b)(6) So let's talk about a federated query on DIVS then.

(b)(6); (b)(7)(C) Sure.

(b)(6) If it's one query that reaches into multiple data sets including the 702 data, is it the same standard for queries across all those different data sets?

(b)(6); (b)(7)(C) It is now. So because the FISA information is one of the repositories that is queried, what you, in effect, have had is that the FISA rules now apply to all of these data sets when you conduct that query. If I conduct a query, and I have authorization to get 702 information as a result of that query, then my query needs to meet the FISA standard regardless of the fact that it might not ping any of the -- bring back any of the 702 information regardless of the fact that I was actually intending, thinking, oh, I'm looking for those CBP records or something else.

So what we have already done, because of the FISA information that's in there, is to make sure that we have this more restrictive regime.

(b)(6) And that's true even for FBI personnel who haven't been trained on the 702 data and so wouldn't have direct return but rather the sort of mediated process with supervisory approval that you described before?

(b)(6); (b)(7)(C) So for FBI personnel for whom the data would not return content or metadata, for those individuals their queries would not necessarily need to meet the standard because one of the things that is in this repository are internal FBI records when someone has done like a temporary duty assignment, but they would, at most, get back a response saying there is positive foreign intelligence -- there is a positive hit in this repository that contains FISA and some other information.

And they would stop there unless they were conducting a foreign intelligence or evidence-of-a-crime-type query, and, in that case, they would have to go to a

(b)(1); (b)(3); (b)(7)(E) [redacted]

(b)(6) But in any scenario, a query that reaches into the 702 data is subject to the reasonably designed to return foreign intelligence information or

evidence of a crime.

(b)(6); (b)(7)(C) If content or metadata can be returned to the person conducting the query, then it has to meet that standard each and every time.

(b)(6) Okay. And if it were withheld from

(b)(1); (b)(3); (b)(7)(E)

[redacted]

(b)(6); (b)(7)(C) Yes.

(b)(6) But they ultimately only get it if it meets that standard after people look at it; is that right?

(b)(6); (b)(7)(C) Correct.

Just one small clarification on that when it talks

(b)(1); (b)(3); (b)(7)(E)

[redacted]

(b)(1); (b)(3); (b)(7)(E)

[redacted]

If the answer is no, it ends there. That information goes nowhere. It doesn't go into FBI's case files. It doesn't go for permanent retention. It isn't disseminated.

If the answer is yes, and it is foreign intelligence information or evidence of a crime, it is covered by the minimization procedures and used appropriately.

(b)(6) Thank you.

One more question. Should it be understood that it's not sufficient for -- in order to run a query that touches on the 702 data, for it to relate to the subject of an assessment or any other type of open FBI investigation, it has to be reasonably designed to return evidence of a crime or foreign intelligence information? So it may be necessary, but it's not sufficient that it relates to an open assessment or other --

(b)(6); (b)(7)(C) Correct.

(b)(6) -- category of case.

(b)(6); (b)(7)(C) Every query that returns content or metadata has to be for an authorized purpose. That authorized purpose has to be that the query is reasonably

designed to return foreign intelligence information or evidence of a crime. That is true for every query that returns content or metadata.

(b)(6) Thank you.

THE COURT: All right. Thank you very much, (b)(6); (b)(7)(C) I appreciate your work on that.

(b)(6); (b)(7)(C) Thank you, Your Honor.

THE COURT: Anything else?

MS. JEFFRESS: No, Your Honor. I think the government may want another word. No?

MR. EVANS: One moment, Your Honor, if you would.

THE COURT: Sure.

(Pause)

MR. EVANS: Your Honor, nothing further. Thank you.

THE COURT: All right. Thank you.

I want to thank you again, all the counsel here, for their work on the matter and the agents, but particularly Ms. Amy Jeffress, who dedicated, I know, weekends and nights to prepare and to study and understand, in a short period of time, this rather difficult and complex area and has given an excellent report of great assistance to the Court, and that's why we have an Amicus. So I appreciate that very much.

We are going to look at this. We have to consider

03:06:53PM 1 the certifications in the near future to look forward on
0: :58PM 2 these matters. So we'll take a look at it, and let you all
03:07:01PM 3 know. Thank you again.
03:07:03PM 4 (Whereupon the hearing was
5 concluded at 3:07 p.m.)
6
7
8
9 **CERTIFICATE OF OFFICIAL COURT REPORTER**
10
11 I, (b)(6) RDR, CRR, do hereby
12 certify that the above and foregoing constitutes a true and
13 accurate transcript of my stenographic notes and is a full,
14 true and complete transcript of the proceedings to the best
15 of my ability.
16 Dated this 29th day of October, 2015.
17 (b)(6)
18
19
20
21
22
23
24
25

All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

~~SECRET//NOFORN~~

2008 AUG 19 PM 3:24
CLERK

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE ATTORNEY GENERAL GUIDELINES ADOPTED PURSUANT TO 50 U.S.C. § 1881a(f)(1). (U)	**UNDER SEAL** Docket No: [redacted]

GOVERNMENT'S EX PARTE SUBMISSION OF ATTORNEY GENERAL GUIDELINES (U)

In accordance with subsection 702(f)(2)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and through the undersigned Department of Justice attorney, hereby submits ex parte the attached "Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as Amended."

~~SECRET//NOFORN~~

~~Classified by:~~ ~~Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ~~
~~Reason:~~ ~~1.4 (c)~~
~~Declassify on:~~ ~~6 August 2033~~

All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

These guidelines have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(f)(1) of the Act. (U)

Respectfully submitted,

(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

National Security Division
United States Department of Justice

ACLU 16-CV-8936 (RMB) 00171

All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

THE ATTORNEY GENERAL'S GUIDELINES FOR THE ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

INTRODUCTION (U)

These guidelines have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(f)(1) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). They govern the implementation of acquisitions of foreign intelligence information under the Act. (U)

ACQUISITIONS UNDER SUBSECTION 702(a) OF THE ACT (U)

All acquisitions conducted under subsection 702(a) of the Act shall be conducted in compliance with the following limitations:

1) **An acquisition authorized under subsection 702(a) of the Act may not *intentionally target any person known at the time of acquisition to be located* in the United States.** The targeting of a person under subsection 702(a) may be done only in accordance with targeting procedures that have been adopted by the Attorney General in consultation with the Director of National Intelligence and that are reasonably designed to ensure that only persons reasonably believed to be located outside the United States are targeted. Any targeting procedures adopted by the Attorney General in consultation with the Director of National Intelligence also shall include measures for detecting those occasions when a person who when targeted was reasonably believed to be located overseas has since entered the United States. Such targeting procedures also shall require that when such an

Classified by: The Attorney General
Reason: 1.4(c)
Declassify on: 1 August 2033

ACLU 16-CV-8936 (RMB) 00172

when such an occasion is detected, all acquisition from the targeted person shall be terminated without delay. ~~(S)~~

2) **An acquisition authorized under subsection 702(a) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States.** A non-United States person reasonably believed to be located outside the United States may not be targeted under subsection 702(a) unless a significant purpose of the targeting is to acquire foreign intelligence information that such person possesses, is reasonably expected to receive, and/or is likely to communicate. ~~(S)~~

If, at any time an agency targets a person, it has as its purpose for targeting that person the targeting of a particular, known person reasonably believed to be in the United States, it must follow the prescribed procedures under the Foreign Intelligence Surveillance Act and other governing authorities that apply for targeting persons inside the U.S. ~~(S)~~

3) **An acquisition authorized under subsection 702(a) may not intentionally target a United States person reasonably believed to be located outside the United States.** Any targeting procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, shall include a requirement that, in targeting a person reasonably believed to be located outside the United States, due diligence is exercised to inform the reasonable belief that the target of the acquisition is not a United States person. [redacted]

[redacted]

~~SECRET//NOFORN~~

[redacted] ~~(S)~~

If, at any time an agency targets a person, it is intentionally targeting a United States person reasonably believed to be outside the United States, it must follow the prescribed procedures under the Foreign Intelligence Surveillance Act and other governing authorities that apply for targeting U.S. persons abroad. ~~(S)~~

4) **An acquisition authorized under subsection 702(a) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.** Any targeting procedures adopted by the Attorney General in consultation with the Director of National Intelligence shall include measures for detecting those occasions when a person who when targeted was reasonably believed to be located overseas has since entered the United States. Such targeting procedures also shall require that when such an occasion is detected, all acquisition from the targeted person shall be terminated without delay. ~~(S)~~

5) **An acquisition authorized under subsection 702(a) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.** Any communication to, from, or concerning a United States person that is incidentally acquired under subsection 702(a) of the Act shall be processed in accordance with minimization procedures which meet the definition of minimization procedures in subsections 101(h) and 301(4) of the Act and

which have been adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. (U)

Any acquisition of foreign intelligence information under subsection 702(a) that does not comply with each of these limitations is prohibited. Furthermore, an acquisition authorized under subsection 702(a) shall be conducted only in accordance with:

1) targeting and minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsections 702(d) and (e) of the Act; and

2) upon submission of a certification in accordance with subsection 702(g) of the Act, such certification. (U)

Specific guidance regarding targeting. Intelligence agencies may not designate a nominal non-U.S. person foreign target when the actual target is a U.S. communicant with whom that foreign target is known to be in contact. [redacted] ~~(S//NF)~~

1) [redacted] ~~(S//NF)~~

2) [redacted]

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

3) [redacted] ~~(S//NF)~~

4) [redacted] ~~(S//NF)~~

ACQUISITIONS FOR WHICH AN APPLICATION FOR A COURT ORDER UNDER THE ACT MUST BE FILED (U)

Any time an element of the Intelligence Community seeks to acquire foreign intelligence information by conducting electronic surveillance, pen register or trap and trace surveillance, or physical search, as defined in the Act, of any person known at the time of acquisition to be located in the United States, an application for a court order under the Act must be filed. Prior to the making of such application, the Attorney General may authorize emergency collection as provided in the Act. (U)

Any time an element of the Intelligence Community seeks to acquire foreign intelligence information by intentionally targeting a United States person reasonably believed to be located outside the United States, and such acquisition is conducted within the United States and constitutes electronic surveillance or the acquisition of [redacted] an application for a court order under the Act must be filed and authority to do so must be obtained from the Attorney General pursuant to Section 2.5 of Executive Order

All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

12333. Prior to the making of such application, the Attorney General may authorize emergency acquisition as provided in the Act. (U)

Any time an element of the Intelligence Community seeks to acquire foreign intelligence information by intentionally targeting a United States person reasonably believed to be located outside the United States under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes, and such acquisition is conducted outside the United States, an application for a court order under the Act must be filed and authority to do so must be obtained from the Attorney General pursuant to Section 2.5 of Executive Order 12333. Prior to the making of such application, the Attorney General may authorize emergency acquisition as provided in the Act. (U)

AUG 5 2008

Date

Michael B. Mukasey
Attorney General of the United States

ACLU 16-CV-8936 (RMB) 00177

Emergency USP Content Queries within FAA 702 PRISM and Telephony Content Collection

External Oversight Process Description

Oversight Activity Name: Emergency USP Queries within FAA 702 PRISM and Telephony Content Collection

Document Classification: TOP SECRET//COMINT//NOFORN

1. Oversight Purpose

The information described below will provide reasonable assurance[1] to DoJ and ODNI that in the event of a national security emergency (e.g., a threat scenario) any USP identifiers used to query FAA 702 PRISM and telephony content collection will be reasonably likely to return foreign intelligence information. The oversight process described below has been reviewed by NSA Leadership, and NSA can reasonably implement it.

2. External Oversight Process

Emergency Scenario: NSA OGC and SID/SV will approve any United States person identifiers used to query the FAA 702 PRISM and telephony content collection. NSA will maintain a specific record of the following information and provide DoJ and ODNI such information for oversight purposes as soon as practicable after approval:

a. Approved identifiers and the realm for each identifier;

b. The United States person, if known, who uses the identifier; and

c. The foreign intelligence information reasonably likely to be obtained by running a query with the identifier, stated as:

- *A short description of the user of the identifier and/or the foreign intelligence information that could be obtained from a query, as well as the basis for this belief; it will not include attachments or supporting analytic assessment documentation.*

Example information:

Identifier	Realm	US Person Name	Foreign Intelligence
[redacted]	[redacted]	[redacted]	[redacted]

[1] "Reasonable assurance" is a term of art commonly used in the auditing and compliance context that serves as an acknowledgment that it is not possible to assert with absolute certainty that an event will or will not occur. In the context of oversight activity, the term indicates that oversight personnel will have access to persuasive evidence that will allow them to reach conclusions about whether the underlying activity conforms to a specified compliance standard.

USP Queries within FAA 702 PRISM and Telephony Content Collection

External Oversight Process Description

Oversight Activity Name: USP Queries of FAA 702 PRISM and Telephony Content Collection

Document Classification: TOP SECRET//COMINT//NOFORN

1. Oversight Purpose

The information described below will provide reasonable assurance[1] to DoJ and ODNI that any USP identifiers used to query FAA 702 PRISM and telephony content collection will be reasonably likely to return foreign intelligence information. The oversight process described below has been reviewed by NSA Leadership, and NSA can reasonably implement it.

2. Proposed External Oversight Process

The external oversight requirements of USP queries within FAA 702 PRISM and telephony content collection will depend on the nature of the USP identifier used to query. Three categories of identifiers and their respective oversight processes are described below.

2.1 **Identifiers Managed by Existing Oversight Processes.** All United States person identifiers authorized for electronic surveillance [redacted] FISA Court Order or RAS-approved under NSA's bulk metadata authorities are approved to query the FAA 702 PRISM and telephony content collection because these identifiers have already been reviewed and assessed to be associated with a foreign power, and hence any query with those identifiers is reasonably likely to return foreign intelligence information.

Approval to query each identifier under section 2.1 will cease upon the expiration or termination of the underlying FISA court authority or RAS approval, whichever is applicable to the approved identifier.

a. [redacted] NSA will use these lists as its record for United States person identifiers authorized for electronic surveillance [redacted] FISA Court Order; these lists will be available to DoJ and ODNI upon request.

b. NSA currently maintains records of all RAS-approved identifiers. This list will be made available to DoJ and ODNI upon request.

2.2 **Identifiers Managed by NSA's Targeting Systems and Associated with 704/705b Targets, US Persons Held Captive, or Emergency Collection.** Any United States person identifiers used by approved 704/705b targets that are managed by NSA's

[1] "Reasonable assurance" is a term of art commonly used in the auditing and compliance context that serves as an acknowledgment that it is not possible to assert with absolute certainty that an event will or will not occur. In the context of oversight activity, the term indicates that oversight personnel will have access to persuasive evidence that will allow them to reach conclusions about whether the underlying activity conforms to a specified compliance standard.

ACLU 16-CV-8936 (RMB) 00179

targeting systems and otherwise not identified in section 2.1 above are approved to query the FAA 702 PRISM and telephony content collection because any query with those identifiers is reasonably likely to return foreign intelligence information. Likewise, any United States person identifier used by a person reasonably believed to be held captive by a foreign power or by a group engaged in international terrorist activities are approved to query the FAA 702 PRISM and telephony content collection when DIRNSA (or Acting DIRNSA) has given specific approval to intentionally intercept or deliberately select communications of or concerning a United States person in accordance with Section 4.A.1.a.3 of the Classified Annex to Department of Defense Procedures under Executive Order 12333. Any United States person identifier used by a person approved for collection by DIRNSA or the Attorney General under SP0018, section 4.1.d. are approved to query the FAA 702 PRISM and telephony content collection.

Approval to query each identifier under section 2.2 will cease upon the expiration or termination of the underlying authority to target the individual or upon NSA's determination that the identifier is no longer used by an authorized target.

For each identifier approved under section 2.2, NSA will maintain a specific record of the following information and provide DoJ and ODNI such information for oversight purposes at the existing 60-day review:

a. Approved identifiers and the realm for each identifier;

b. The name of the United States person, if known, who uses the identifier; and

c. The basis for NSA assessing that the identifier is used by an approved 704/705b target, that the identifier is used by a person reasonably believed to be held captive by a foreign power or group engaged in international terrorist activities and has been approved by DIRNSA (or Acting DIRNSA) in accordance with Section 4.A.1.a.3 of the Classified Annex, or that the identifier is used by a person approved for collection by DIRNSA or the Attorney General under SP0018, section 4.1.d. In each of these instances, once the connection to the target is identified, it is clear that foreign intelligence information is reasonably likely to be returned.

Example information:

Identifier	Realm	US Person Name	Foreign Intelligence
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

			[redacted]

2.3 **All Other US Person Identifiers:** For any United States person identifiers approved to query the FAA 702 PRISM and telephony content collection not identified in sections 2.1 and 2.2 above, NSA will maintain a specific record of the following information and provide DoJ and ODNI such information for oversight purposes at the existing 60-day review:

a. Approved identifiers, the realm for each identifier, and the duration of the approval[2];

b. The United States person, if known, who uses the identifier; and

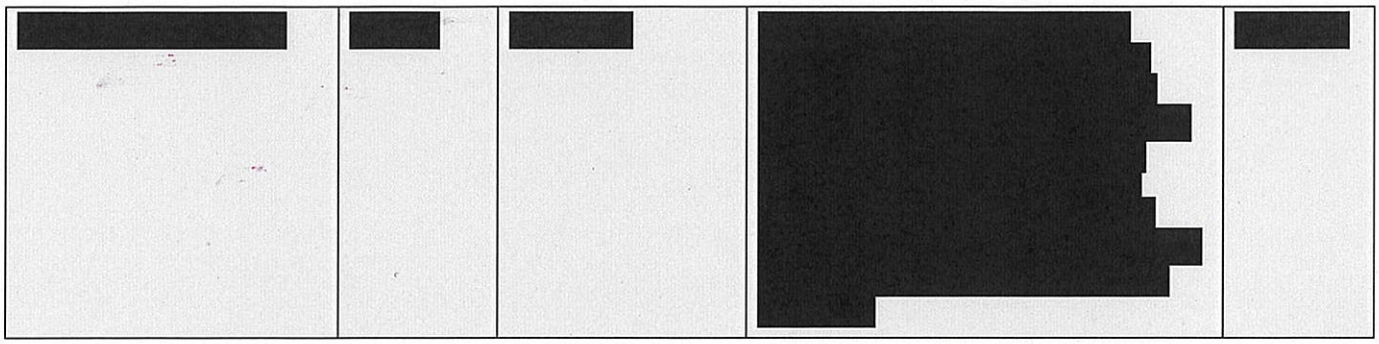
c. The foreign intelligence information reasonably likely to be obtained by running a query with the identifier, stated as:

- *A short description of the user of the identifier and/or the foreign intelligence information that could be obtained from a query, as well as the basis for this belief; it will not include attachments or supporting analytic assessment documentation.*

Example information:

Identifier	Realm	US Person Name	Foreign Intelligence	Duration
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[2] Upon approval of each identifier under section 2.3, the approving official will specify the duration of the approval. The process for managing approvals and durations will be developed as described in Section 3.3.



3. NSA Resources Required to Implement:

Phase I

3.1 (b)(1); (b)(3); (b)(5)

3.2 (b)(1); (b)(3); (b)(5)

Phase II

3.3 (b)(1); (b)(3); (b)(5)

Phase III

3.4 (b)(1); (b)(3); (b)(5)

Technical Implementation

3.5 NSA's technical implementation will allow analysts to define the appropriate parameters to query FAA 702 PRISM and telephony content collection with USP identifiers and not query FAA 702 Upstream collection.

Training

3.6 Additionally, for all phases of implementation, a *USP Query of 702 PRISM and Telephony Content Collection* training package will need to be developed and implemented for both NSA auditors and analysts. This training will cover the information analysts need to document in order to have USP identifiers approved to query FAA 702 PRISM and telephony content collection. (Note: This may be done via email and/or in-person sessions until such information can be included in standard formal training documentation.)

4. Additional Comments:

4.1 Upon request, NSA will make available to DoJ and ODNI any query logs of USP queries of FAA 702 PRISM and telephony content collection that are generated by systems used to query FAA 702 PRISM and telephony content collection.

4.2 It is important to note that a query of the 702 PRISM and telephony content collection may be comprised of several terms, [redacted] these combined terms are utilized to narrow the query results, and minimize the return of irrelevant data. Analysts are already instructed as part of their USSID SP0018 training to make their queries as focused as possible, and NSA auditors are trained to look out for and question analysts regarding overly broad queries. If a USP identifier is included as part of a broader query involving multiple terms, that identifier will still be included in the oversight process described above.

4.3 In general, NSA will be deemed to have met its obligation to support oversight of USP queries of FAA 702 PRISM and telephony content collection under Section 2 above by providing the information described in that section, and will not generally be expected to provide additional supporting documentation or references to specific traffic or reporting. Further, for queries in accordance with sections 2.2.c and 2.3.c above, NSA expects the information descriptions to remain generally consistent with the examples above. Importantly, for queries in accordance with section 2.2, NSA does not intend to require regular updates to the date of the information referenced (e.g., SIGINT collection from October 2011).

4.4 **USP Queries of FAA 702 Metadata**. Oversight of queries of metadata derived from FAA 702 PRISM and telephony collection containing USP identifiers will be handled in accordance with separate procedures. Those queries will not be handled in accordance with these procedures.

Approved for Public Release

U.S. Department of Justice

National Security Division

Washington, D.C. 20530

To: Litigation Section, Office of Intelligence

From: Stuart J. Evans
Deputy Assistant Attorney General for Intelligence

Re: Restriction Regarding the Use of FISA Section 702 Information in Criminal Proceedings Against United States Persons

This memorandum serves to document a policy restriction imposed on authorizations of the use of information acquired from Section 702 of the Foreign Intelligence Surveillance Act (FISA) against United States persons in criminal proceedings.

For background, in January 2014, in response to a recommendation from the President's Review Group on Intelligence and Communication Technologies, the President directed the Attorney General and Director of National Intelligence to place additional restrictions on the government's ability to use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702. The Department of Justice and the Intelligence Community, in consultation with the Administration, subsequently adopted a policy restriction, which was announced in the Intelligence Community's Signals Intelligence Reform 2015 Anniversary Report, published on February 3, 2015. While this restriction was formalized in February 2015, it is also fully consistent with the Department's past practice regarding authorizations for the use of Section 702 acquired information.

Specifically, in addition to any other limitations imposed by applicable law, including FISA, any communication to or from, or information about, a U.S. person acquired under Section 702 of FISA shall not be introduced as evidence against that U.S. person in any criminal proceeding except:

(1) with the prior approval of the Attorney General, and

(2) in

(A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity), or
(B) other prosecutions of crimes involving
(i) death;

(ii) kidnapping;
(iii) substantial bodily harm;
(iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 U.S.C. § 16911;
(v) incapacitation or destruction of critical infrastructure as defined in 42 U.S.C. § 5195c(e);
(vi) cybersecurity;
(vii) transnational crime; or
(viii) human trafficking.

Requests for authority to use Section 702 acquisitions in criminal proceedings against United States persons must comply with the above restriction. Prior to recommending that the Attorney General, as defined by FISA, authorize such use, Office of Intelligence personnel will ensure that the requested use and the recommended authorization complies with the above policy. This policy will remain in effect unless modified in the future by the Attorney General and Director of National Intelligence.

This policy is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.

Cc: Deputy Assistant Attorneys General, National Security Division
Chief, Counterterrorism Section
Chief, Counterintelligence and Export Control Section

USP Queries of Communications Metadata Derived from FAA 702 (b)(3) and Telephony Collection

External Oversight Process Description

(Note: Documented herein is the purpose, process, and implementation details associated with an NSA SIGINT activity that requires external oversight. The formal articulation of these oversight aspects, when combined with the process of coordinating these activities with our overseers will ensure clear understanding between NSA and our overseers regarding oversight expectations. This process will also serve to document NSA's effort and resource allocation required to support the oversight.)

Oversight Activity Name: USP Queries of Communications Metadata derived from FAA 702 (b)(3) and Telephony Collection

Document Classification: TOP SECRET//COMINT//NOFORN

1. Oversight Purpose

The information described below will provide reasonable assurance[1] to DoJ and ODNI that any query of communications metadata derived from FAA 702 (b)(3) and telephony collection starting with USP identifiers will be reasonably likely to return foreign intelligence information. The oversight process described below has been reviewed by NSA Leadership, and NSA can reasonably implement it.

2. Proposed External Oversight Process

2.1 **US Person Identifiers:** For any query of communications metadata[2] derived from the FAA 702 (b)(3) and telephony collection starting with a United States person identifier[3], NSA will maintain a specific record identifying each United States person query, which will include the following information and provide DoJ and ODNI access to such information for oversight purposes at the existing 60-day review:

a. The query; and

b. The foreign intelligence (FI) justification for the query;

i. Each initial (seed) query will require the analyst to enter an FI justification. The FI justification will apply to all traffic analysis performed as a result of

[1] "Reasonable assurance" is a term of art commonly used in the auditing and compliance context that serves as an acknowledgment that it is not possible to assert with absolute certainty that an event will or will not occur. In the context of oversight activity, the term indicates that oversight personnel will have access to persuasive evidence that will allow them to reach conclusions about whether the underlying activity conforms to a specified compliance standard.

[2] For the purpose of these procedures, "communications metadata" is the same as the description of "metadata" provided in the response to question 9 within the Government's Responses to FISC Questions re: Amended 2011 Section 702 Certifications, filed on November 15, 2011, pages 3-8.

[3] NSA will rely on an algorithm and/or a business rule to identify queries of communications metadata derived from the FAA 702 (b)(3) and telephony collection that start with a United States person identifier. Neither method will identify those queries that start with a United States person identifier with 100 percent accuracy.

the seed query, to include the identification and analysis of direct and indirect contacts of the initial (seed) query.

ii. Recording FI justifications is intended to assist NSA/CSS analysts in memorializing the purpose of their metadata analysis activities. The FI justification documents the analytic knowledge linking the selector to a foreign target or foreign intelligence purpose. The FI justification is a memory aid in the event that the analytic process is questioned long after the fact. The justification preserves the rationale behind the query. FI justifications are subject to review (spot check).

3. NSA Resources Required to Implement:

Technical Implementation

3.1 NSA's technical implementation will ensure that USP metadata queries of FAA 702 collection will only run against communications metadata derived from FAA 702 (b)(3) and telephony collection. NSA's Technical Directorate (TD) continues work to implement this requirement.

Training

3.2 Training sufficient to grant analyst access to systems that support the Supplemental Procedures Concerning Communications Metadata Analysis (SPCMA) will be sufficient to start a query of communications metadata derived from FAA 702 (b)(3) and telephony collection with a United States person identifier.

4. Additional Comments:

4.1 (b)(1); (b)(3)

4.2 Analysts are not required to check any specific database or seek any internal approvals prior to executing a query against metadata derived from FAA 702 (b)(3) or telephony collection. Further, NSA analysts are not required to attach supporting documentation to the FI justification or reference specific traffic or reporting.

4.3 These procedures describe the external oversight of USP queries of communications metadata derived from FAA 702 (b)(3) and telephony collection. Nothing in these procedures is intended to alter or modify the underlying minimization procedures NSA personnel apply to the analysis of communications metadata derived from FAA 702 (b)(3) and telephony collection. Substantively, the analysis of FAA 702 (b)(3) and telephony communications metadata does not differ in any material respect from the analysis of metadata governed by the SPCMA procedures that the Secretary of Defense and Attorney General approved in late 2007. Maintaining consistency between the analysis of FAA 702 (b)(3) and telephony metadata and the analysis of metadata governed by the SPCMA process creates a more uniform rule-set for analysts to follow which allows analysts to execute the mission more efficiently and helps prevent compliance incidents.