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

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

[redacted]

HONORABLE THOMAS F. HOGAN, PRESIDING

Friday, August 4, 2014

11:00 a.m.

KEVIN O'CONNOR

FRIDAY, AUGUST 4, 2014

11:23 a.m.

THE COURTROOM CLERK: The case now before the Court is [redacted]. And would everyone please state your names first? We can start at this end.

MR. EVANS: Stuart Evans, Department of Justice.

MR. O'CONNOR: Kevin O'Connor, Department of Justice.

[redacted], Department of Justice.

[redacted], Federal Bureau of Investigation.

MR. DeLONG: John DeLong, National Security Agency.

MR. [redacted]: [redacted], National Security Agency.

MR. [redacted]: [redacted], National Security Agency.

MS. [redacted]: [redacted], National Security Agency.

MR. [redacted]: [redacted], National Security Agency.

MR. [redacted]: [redacted], National Security Agency.

[redacted], Federal Bureau of Investigation.

[redacted] Office of the Director of National Intelligence.

(b)(6) [redacted]

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

Department of Justice.

THE COURT: All right. Thank you. Please be seated.

THE COURTROOM CLERK: Would you like me to place anyone under oath?

THE COURT: Not right this minute. We might. All right. Thank you all for coming in. We've spent some time reviewing these applications on the certifications for the 702 requirements, that each year we meet to consider these overall. I'm sure that the targeting agency procedures are appropriate. They're complicated certifications. We've looked through those and I know that the staff has had an opportunity to work with you all on these matters as well, and I -- I have several questions and issues I'd like to discuss. A lot has -- the government has, through its communications with the staff, I think, has edited much of these to make sure they meet the requirements of the statute.

There had been, obviously, some compliance issues we'll talk about a little bit, I hope, and get into what happened, as well as some of the changes in the minimization procedures that you all are looking at.

I thought there were a couple of areas I wanted to hear, and maybe [redacted] is the one to start with this, in the overall areas a couple of matters that have been raised with me.

Is it in the -- the targeting procedures across the board,

I think, are going to be very applicable to each of the agencies at this point, and I know you're aware that Judge Mosman had a case or cases that came up with some issues and whether or not there are procedures, in fact, on how you go about, now each of the agencies, in determining if a person is a U.S. person under the procedures or not, and how you determine that, [redacted]. So where are you on that? Maybe we can talk about that. Who's the expert for me?

MR. O'CONNOR: Thank you, Your Honor. I'm Kevin O'Connor with the Department of Justice. I'm chief of the Oversight Section within the National Security Division. To your question of the efforts that each of the agencies takes to ensure that 702 targets are not U.S. persons, each of the agencies recognize that if they are faced with information that indicates that a target or potential target may be a U.S. person, its incumbent upon them to address and satisfy themselves that those questions are, in fact, answered.

THE COURT: [redacted]

MR. O'CONNOR: [redacted]

[redacted]

THE COURT: In [redacted]

[redacted]

MR. O'CONNOR: [redacted]

[redacted]

Looking historically, the government has -- had very few instances in which the U.S. person determination under 702 was, in fact, incorrect. [redacted] issues, the agencies and the department and ODNI have had a discussion about ensuring that those who are making the targeting decisions recognize instances in which there is a legitimate question regarding U.S. person status that needs to be resolved, and they are -- have gotten word to their analysts and agents and targeters that there are situations [redacted]

[redacted]

MR. O'CONNOR: [redacted]

THE COURT: All right. Each of the agencies now in these minimization procedures will make their own checks, as I understand it, to make sure it's a non-U.S. citizen that's being targeted, and NSA will do the [redacted] to determine in the task for electronic communications is accessed within the U.S., but each agency will do its own, as I understand, check to

see that they're targeting a non-U.S. person?

MR. O'CONNOR: To the extent that NSA is responsible for [redacted], it's incumbent upon the NSA to make that determination that the target is an appropriate target under 702, to assess the full U.S. as well as the non-U.S. status.

When the FBI [redacted], the FBI will undertake efforts to determine whether they possess any information that is contrary to the determination made by the NSA. [redacted] it will undertake to continually assess and monitor those communications for any indication that the individual has roamed into the United States, was initially in the United States, or, in fact, is a U.S. person.

THE COURT: Tell me a little bit of background. You said this was really unusual, the [redacted] that came up. When you're saying "unusual," meaning there were [redacted] you know that this has happened?

MR. O'CONNOR: Under those particular circumstances, yes, Your Honor. There have been certainly other instances in which a determination was made that [redacted], but those instances are few and far between.

THE COURT: Now, in each of the -- as to each of these agencies, then, you have clarified their obligations, as I

understand it; is that correct, in these certifications?

MR. O'CONNOR: Yes, Your Honor, and I've attempted to explain the approach that each of the agencies take to these types of situations.

THE COURT: All right. All right, Mr. O'Connor, thank you. Let me talk to you a little bit about, as we go through, these changes. On some of the minimization procedures, one of the big changes to me, it seems to me, is the retention of information usually subject to destruction or age-off requirements, and I would like a little bit of an explanation on that and how you intend to follow that up with the agencies to -- and how the government intends to coordinate it with the other branches of the Justice Department that may be involved in this litigation to know whether or not they are supposed to be retaining information, because I know in the past it's caused some difficulties.

[redacted] [redacted] Good morning, Your Honor. [redacted]

So, the Court is correct, each of the agency's minimization procedures that are currently before the Court now have language in them that would permit the agencies to retain information that would otherwise be subject to age-off in the event a litigation matter arises that would require retention. Previously none of the agencies' procedures had this provision in it.

THE COURT: You had to come here?

[redacted]: That's correct. And we've had this crop up in a couple of different circumstances. (b)(1); (b)(3); (b)(7)(E) [redacted] (b)(1); (b)(3); (b)(7)(E) --

THE COURT: -- yes --

[redacted]: -- where we've had to come in one-off cases to the Court and seek a departure from (b)(1); (b)(3); (b)(7)(E) [redacted] in order to accommodate that.

The other circumstance where this occurred recently was not in the 702 context, but was in what we call the big business record context where, as the Court's aware, all of the primary orders which deal with how data is to be handled and retained and disposed of had a five-year retention limit. We were coming up on that five-year retention limit, and as a result of some civil litigation out in California where the Department made a determination that in order to comply with the District Court's preservation order out there, we needed to be able to retain that data for longer than five years, so we presented a motion to Judge Walton which he analyzed and granted. So those were some of the circumstances that we've confronted to date.

Just to round that out for the Court a little bit more, the litigation in California continues. The litigation in California has the potential to include data other than the data that has been retained under the big business records program to include potentially 702 data. Those matters are still being

litigated, but as a result of that, we wanted to have a mechanism in place so that if we determine that we need to retain data, the minimization procedures contemplate that.

One of the differences with respect to the way 702 works versus Titles I and III of FISA where we could come in individual cases a lot more -- with a lot more agility and seek individual departures. In the 702 context, in order to change minimization procedures, the Attorney General and the DNI have to execute amended certifications with amended minimization procedures that then have to be presented to the Court. So it's a much more cumbersome process, and when you're faced with impending preservation obligations in another court, that could potentially put us at odds with obligations in other cases.

So, in light of that, we've developed procedures for each of the agencies to allow them to retain data that would otherwise be subject to age-off. In circumstances where the agencies working with the department receive from the Department in writing a notification that a decision has been made that certain information is subject to preservation, what the case is, where that obligation arises, what the scope of the information is that will be retained, and then subsequently, if it's ultimately decided that the information no longer needs to be retained, another written notice to the agency telling them, "Your preservation obligation has been lifted and it's now appropriate for you to destroy the data consistent with your minimization

procedures."

So, in each circumstance where this would arise going forward, it would not be a circumstance where the agency independent of the Department would be making decisions about what to retain or what not to retain, it would be a collaborative effort ultimately ending up with the Department actually telling the agency what they needed to keep.

THE COURT: And you've got some system of coordinating these cases that are coming up, this general litigation over the FISA-type work where you all are notified from the civil division of the Justice Department or whoever is handling it at the Justice Department, because sometimes there's a gap there, you know.

[redacted]: So there are a fair number of cases that are out there. I think by last count, although don't hold me to this, it was in excess of [redacted] either FOIA cases or civil litigation cases that are out there. The civil cases, we work closely with the relevant parts of the civil division in those cases as a general matter in, you know, answering complaints, in drafting briefs and things like that. In the civil division, as new cases come in, they tell us the new cases have come in and we coordinate with them.

In the criminal context, this is where the collaboration comes in, because it may be that if a criminal matter is being handled in a U.S. Attorney's Office in the district of Idaho, NSD

may not be witting of that, but an agency may get some type of a notification from that U.S. Attorney's Office, and so that's where the collaborative effort comes in. If an agency would get a notification like that, they would notify us, and then we would work with them to develop whatever the approach was that would be necessary for retention in those kinds of cases. If it's a terrorism matter (b)(1); (b)(3); (b)(7)(E) that would be handled within the division, (b)(1); (b)(3); (b)(7)(E) the counterterrorism section [redacted] we would be working within the division to make sure we were witting of those kinds of cases.

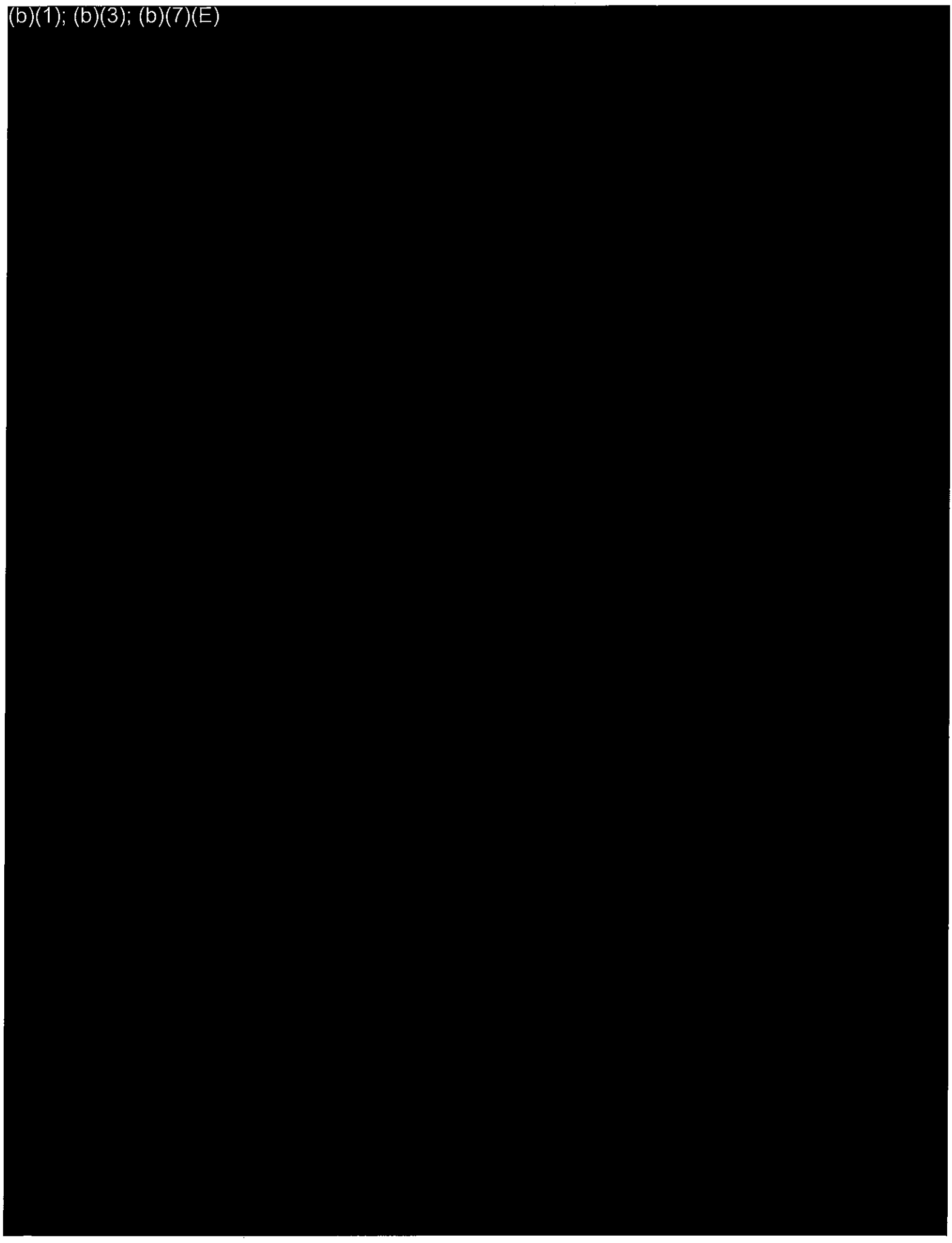
THE COURT: And each of the agencies have effectively signed on to this? They understand?

(b)(6); (b)(7)(C) [redacted]: We have had detailed discussions with them about how this would work. They can obviously acknowledge, but I am comfortable that they understand how this process will work.

THE COURT: It makes sense, I mean all the sense in the world, rather than, as you said, trying to come back to us with the Attorney General trying to change minimization procedures when this litigation is now becoming fairly prevalent in the country and has caused difficulties in other contexts for the government with the court.

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

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



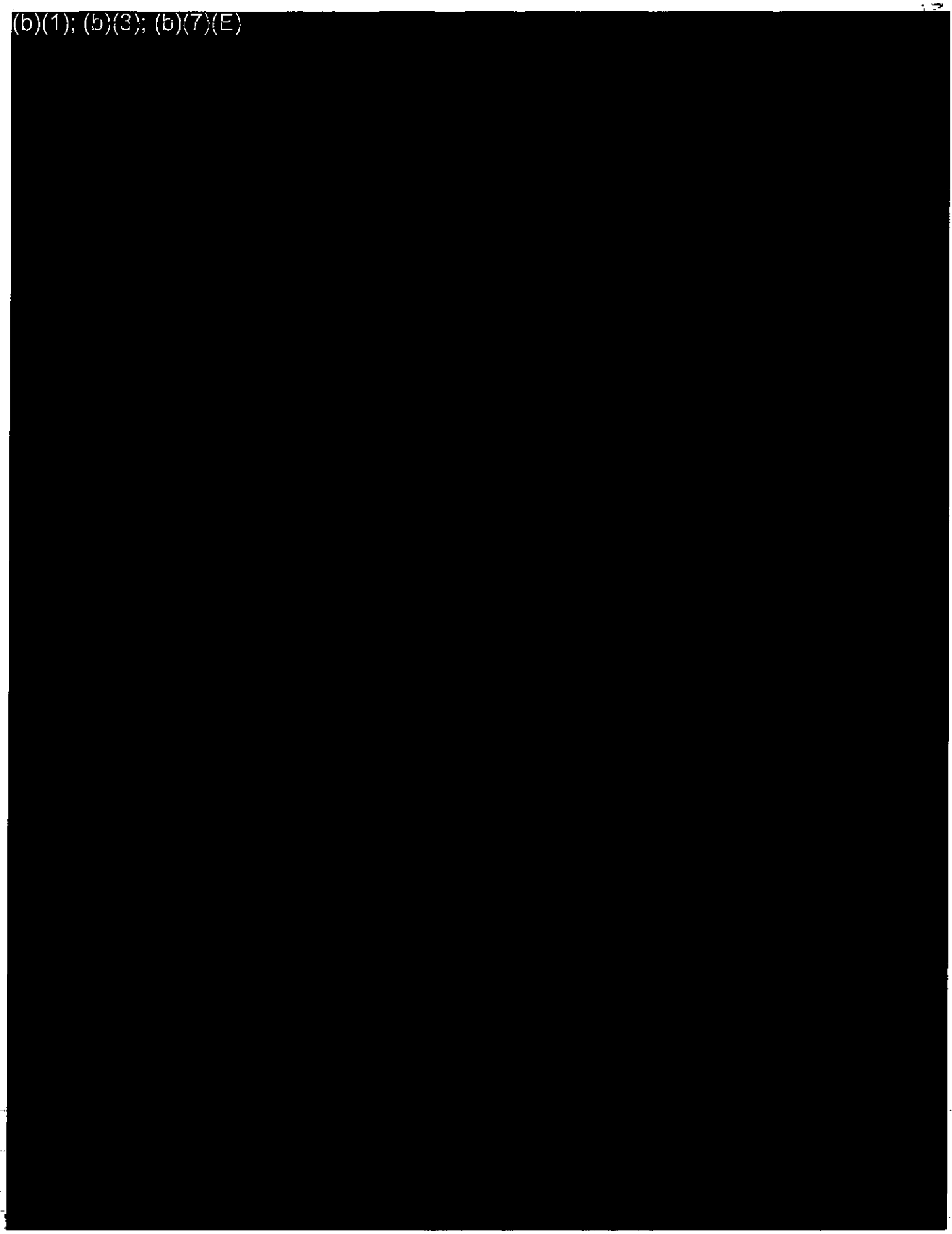
(b)(1); (b)(3); (b)(7)(E)

[redacted]

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

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

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



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

[redacted]

THE COURT: You mentioned the other minimization procedures in this area that was suggested, and that is the sharing with private individuals for mitigating serious economic harm or serious physical injury. What's, like, an economic harm that would apply to? What's an example?

(b)(6); (b)(7)(C) [redacted] So, the best example that I can give you is

the one that we gave to the Attorney General when we gave him the procedures. (b)(1); (b)(3); (b)(7)(E) [redacted]

THE COURT: And if you use any of these procedures, you or [redacted] and advising them of other matters or apprising other individuals of threats of serious economic harm or physical injury to life or property, is there any provisions for reporting back to the Court on how many times this occurs or anything like that? Do we have any idea how broad spread or widespread this may be?

[redacted] So that was something that we thought about, and in the procedures dealing with serious economic or physical harm, there's a requirement to report back to the Department within ten days of exercising that authority. They are not similar requirements in the [redacted] portions of the procedures or the cyber portions of the procedures.

I would say, though, that if that's something that the Court is concerned about, we could certainly work with the Court

and its staff to come up with a way to provide the Court with information if disseminations are made pursuant to those provisions.

THE COURT: There's some pending legislation. I don't know if they need more work, but we'll think about that.

[redacted] We'll certainly be in touch with the staff on those issues.

THE COURT: All right. Thank you. Other minimization procedures suggest, I think. Actually there are some very good changes you've made, and I don't see too many questions about them. We have some compliance instances I need to talk about, other areas, but the [redacted] concerned me, and I'll get back to Mr. O'Connor in a second on that if I have any further questions about it, and I do think that the idea of adding in the retention capabilities is important in this area.

The use of [redacted] as a possibility, I've got to look at a little bit more, make sure that that's appropriate, and I think the notice of some serious economic concerns or physical danger is sensible, as long as it's properly done, obviously, and I'm making these applicable across the board, I think is very important, so we don't have differences among the agencies how these are being operated. Let me ask Mr. O'Connor back, if he can get back in the hot seat again.

And I just want to make sure I'm checking on whether or not this tasking, before it begins, is not a U.S. person, that

all of the -- that is the CIA and the FBI and NSA -- [redacted] And if not, because they're satisfied with what they have, is there any idea we should require them to always go beyond that and make sure that they aren't targeting U.S. citizens.

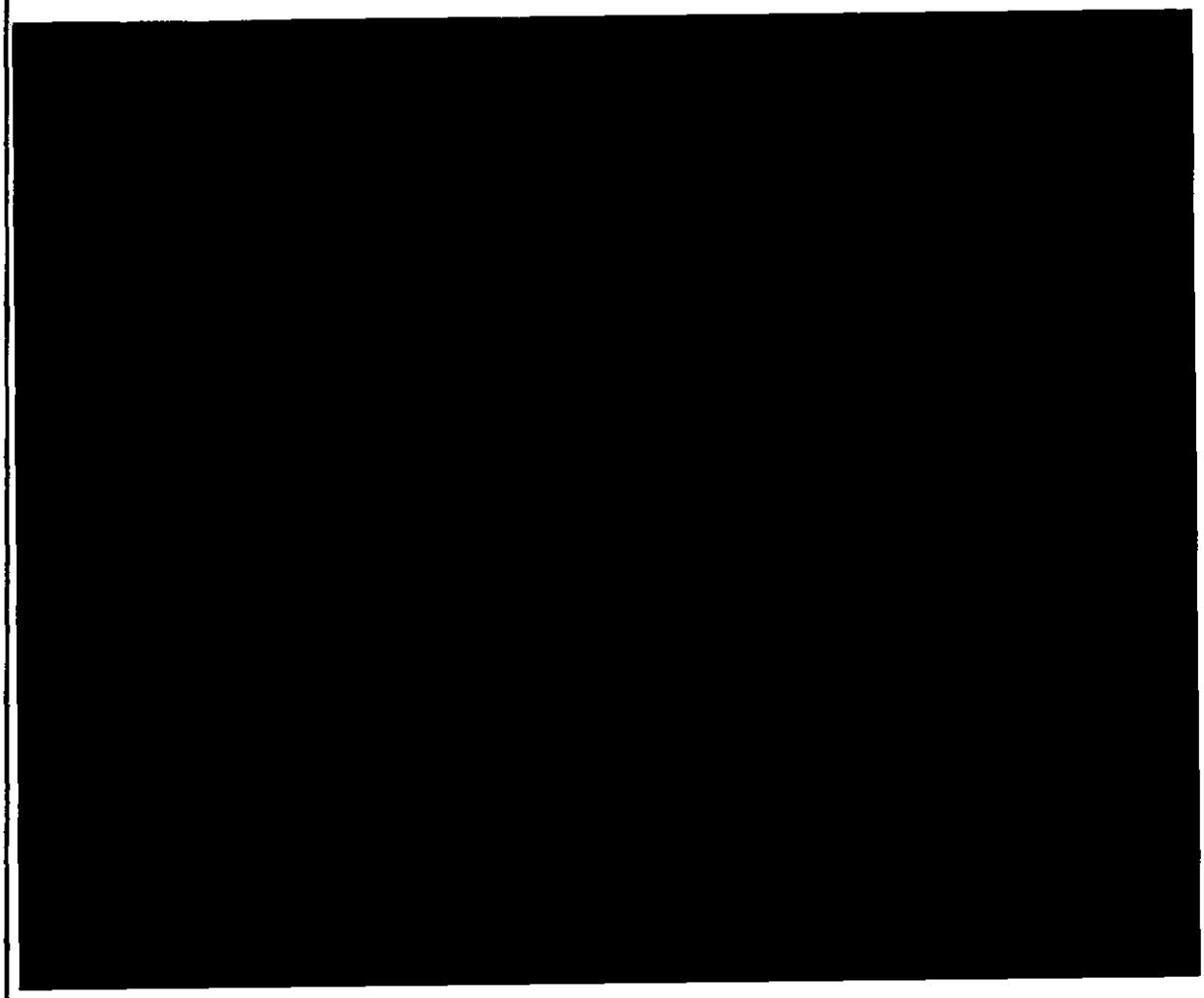
MR. O'CONNOR: In answering --

THE COURT: You answered, [redacted].

MR. O'CONNOR: So, in most circumstances, Your Honor, I think that the government would posit [redacted] in most instances they're able to establish a reasonable basis to believe that an individual's a non-U.S. person [redacted]. It's those circumstances in which there is a real and substantial question where they have information indicating that the target may be a U.S. person and are unable to resolve that [redacted] But in the vast majority of circumstances, the agencies are able to satisfactorily answer that question [redacted]

THE COURT: What happened [redacted]? How did that occur?

MR. O'CONNOR: [redacted]



THE COURT: And so the same procedures are followed then by the NSA and the FBI?

MR. O'CONNOR: My understanding is that the NSA has adopted similar guidance for its targeters, and the FBI as well is assessing how best to get the message out to their folks to make that message clear.

THE COURT: I don't know if you want to do this or if the FBI wants to talk about some issues on compliance, one, the recent confusion and notices regarding instances where case agents reviewing 702 collection material against a target knew

that he was under indictment and there may be attorney-client privileged questions and that wasn't caught, and I got advice that that was a mistake and a note that was inaccurate, and then I got an advice, when they came in Friday or yesterday, even over the weekend maybe, that no, there were other additions, [redacted] like this this year.

MR. O'CONNOR: Yes, Your Honor. If I might take a stab at answering your questions, and if necessary, with the leave of the Court, we'll ask the FBI to come in and fill in any additional details you might want to hear about.

There are [redacted] circumstances that I'd like to inform the Court about for which notices have not yet been filed, each of which involve 702 targets that were subject to charges in the United States where collection continued and a taint team was not put in place as required by the minimization procedures.

[redacted]

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

[redacted]

Now, the FBI, along with NSD, are putting in place several measures. I'm happy to detail those for you, Your Honor, to ensure that across the board the agents and analysts and attorneys involved in the review of 702 collection understand and are able to apply the attorney-client communications provisions of the SMPs.

THE COURT: Yeah. I mean, there seems to be several just recently -- maybe that's because they're ramping up some terrorist prosecutions that's going to occur, but you advise these on a quarterly basis if we have these.

MR. O'CONNOR: We can do that Your Honor, yes, or we do do that, Your Honor.

THE COURT: Or outside of that. I just -- it concerns me if this is going to keep up -- obviously, I assume the FBI is going to go back to its agents and talk a little bit about enhancing their training in this area. I think it would be of help because I'm very concerned you're going to run into a real buzz saw if you have any attorney-client communications there and it becomes known. It's something that we have to be careful about if we're going to have this go on.

Other areas of compliance from the purging areas in the FBI. You had several of those about the report, again, that we just received, I think [redacted] FISA court information over multiple databases and trying to track that down and making sure that the -- they may not have been exported. And what have you done and how have you done that? Has there been any effort to go back and track down these queries that have been made and see what's happened or not?

MR. O'CONNOR: So, Your Honor, generally the issue there, to recap, is an agent can conduct a query in an FBI database and explore those query results. The database oftentimes will have a query log. The FBI had not incorporated a review of those query logs as part of this purge process. The FBI has since done that. Historically, there's no way for the FBI to go and assure itself that none of those exported results were, in fact, disseminated.

What the FBI has done is looked historically and determined that the FBI had very few instances in which 702 collection was required to be purged and looked at the nature and the use of the agents of that export function, which is typically for internal analytics as opposed to exporting for the purpose of dissemination.

THE COURT: And are you satisfied that you're caught up with this problem at this point?

MR. O'CONNOR: Yes, Your Honor, the FBI has analyzed it and modified its purge process to account for this export function in the databases.

THE COURT: All right. How about NSA purging issues that you had advised us about concerning its compliance in [redacted] and maybe an overview by NSA on what they've done to ensure that these purging processes have worked out effectively, that -- whether or not it's human error and there's training going on or there's more electronic changes that need to be made in the systems. I mean, just a description of where we are with that.

MR. O'CONNOR: Yes, Your Honor, with the Court's permission, I would like to introduce John DeLong, the Director of Compliance for NSA, to address your questions.

THE COURT: Sure. I'm referring to July 1 or the July 25th letter that set out a couple of these issues for us and another one back in March, you gave us another report.

MR. DeLONG: Your Honor, John DeLong. So I think there's two questions, at least, that we had gotten a little bit more detail from the court advisors from Justice. One was the disposition of the study [redacted]. So, with your permission, I'll cover that at the general level. And we also have [redacted] here who leads the 702 purge team, if the Court has any additional questions. And then I think again, maybe a little bit of a deeper dive into some of the additional safeguards that exist for purge.

THE COURT: All right.

MR. DeLONG: With your permission, I'll proceed in that way. So, on the [redacted], as we reported to you, we were -- we went ahead and ran the full MPL against the [redacted] database. Because there was a triggering event, we decided that that would be a good way to more fully understand, get to root causes. We have received those results, we've binned them in essentially root cause cases.

In many of those cases, improvements in the intervening time between when those objects -- you know, essentially already addressed those root causes, so we did not make any additional changes because of those root causes. In some cases, especially due to the interaction that gave rise to that [redacted] garble, we obviously took steps to more appropriately match up items that are on [redacted] with the way they're described in the database. [redacted]

[redacted]

So, you know, technically it has to do with different types of [redacted] but if the Court would like we can get into that, but the short story is we've addressed that and as a result the root causes have essentially been through those, worked them off -- Like I said, many of them had already been worked off just through intervening events and improved safeguards. The ones that arose from the [redacted] incident we've also addressed.

THE COURT: What -- I mean, what is sort of the schedule you're working under on being in compliance with the purge procedures? I mean, one of the letters I looked at that you note here you indicated that [redacted]

MR. DeLONG: A little clarification, if I might Your Honor. So we have a [redacted], as has been described to the Court. We can and do run that occasionally for certain reasons across our systems. As you know, we have a purged taxonomy. We divided our systems into different categories. [redacted]

[redacted]

[redacted].

In 2010, before we certified systems as source systems of record, the [redacted] we had in 2010, we've added [redacted] since. We also ran the entire Master Purge List through those systems. [redacted] And obviously, as you saw in the [redacted] incident, when there's a triggering event, we run the MPL.

So I guess to raise the question and then answer the question, the question may be, why not, as a matter of course, run the entire, full Master Purge List across all our systems on a, let's say, routine basis? If that's the question, I understand, Your Honor, and I might go ahead and address that.

THE COURT: Yes, and then -- I guess my basic question is what assurance do you get or not running searches on information that's supposed to have been purged.

MR. DeLONG: Absolutely. So again, as described in the letters, and maybe I'll go back to 2010. So in 2010 we did a one time run. We also in May 2010 -- May 26th letter described a series of testing and independent auditing that we would be doing, and so much of what has gone on since then has been consistent with that promise in 2010.

The -- at the 10,000 foot level, running the full MPL across all the systems is not the best return on investment for

the purpose for which it might be applied, [redacted]

[redacted] And so in many of those cases -- and again, there are a variety. Obviously, the 702 purges are a constant, daily activity. [redacted], just as an example. I just need to use examples here.

So what happens is, number one, running the MPL against the [redacted] is both an intense process for the system that takes time and energy and -- it's also an investment. When you invest in something to get a good return, anything you invest in, what it then does is it generates a lot of false positive, if you may, it generates a lot

of work. The running down of the Master Purge List is not -- because it's optimized for, you know, [redacted] and that then takes a lot of time and energy from the purge team.

So basically, and we would respectfully submit, if running the full MPL against all the systems on periodic basis doesn't generate the best return on investment, what would? And so what we do -- [redacted], there's a lot of different ways to skin the cat, if you will. What we've determined in our best judgment is that doing a statistical sample of the Master Purge List on a routine basis and running it against the systems and seeing those results -- and again, this is drawing from principles of internal auditing. It's a tried and true method. It helps us diagnosis process errors. Each of those we then run down, and I think as you you've seen in the letters, in 2011 and 2012 and 2013, we've seen trends in a positive direction. By that I mean closer to zero. If we were to see trends going up, that might trigger a series of follow-on events. So I don't know if that answers your questions.

THE COURT: Yeah, that's helpful. You mentioned root causes. What's a root cause?

MR. DeLONG: A root cause may be -- for example, we used to use e-mail to deliver -- [redacted], we made a decision in 2010 that the purge team would communicate directly with those systems, [redacted] Those communications in some cases were done through e-mail. Sometimes we could find a record where maybe an e-mail was sent but maybe not received. That might be a root cause. There's some incomplete nature of e-mail. You know, you might get a return receipt, but it might not have actually been read or not followed on. So in those cases, in some cases now, we don't use e-mail to communicate anymore between the systems. We have a much more direct interface. And, in fact, we had a few garbles as we changed over to that interface, but the impact of that is much better, so that would be an example of a root cause. The other one that was more [redacted] and I would like to address to see if there are any additional comments was that kind of [redacted]

THE COURT: Thank you, Mr. DeLong, I appreciate it.

One of the other matters that I just wanted to double-check on a little bit was the collaboration between the

NSA [redacted]. Who wants to talk about that? Who's knowledgeable on the NSA's collaboration?

(b)(6); (b)(7)(C) [redacted] I'll start, Your Honor. (b)(6); (b)(7)(C) again, and if you get really down in the weeds --

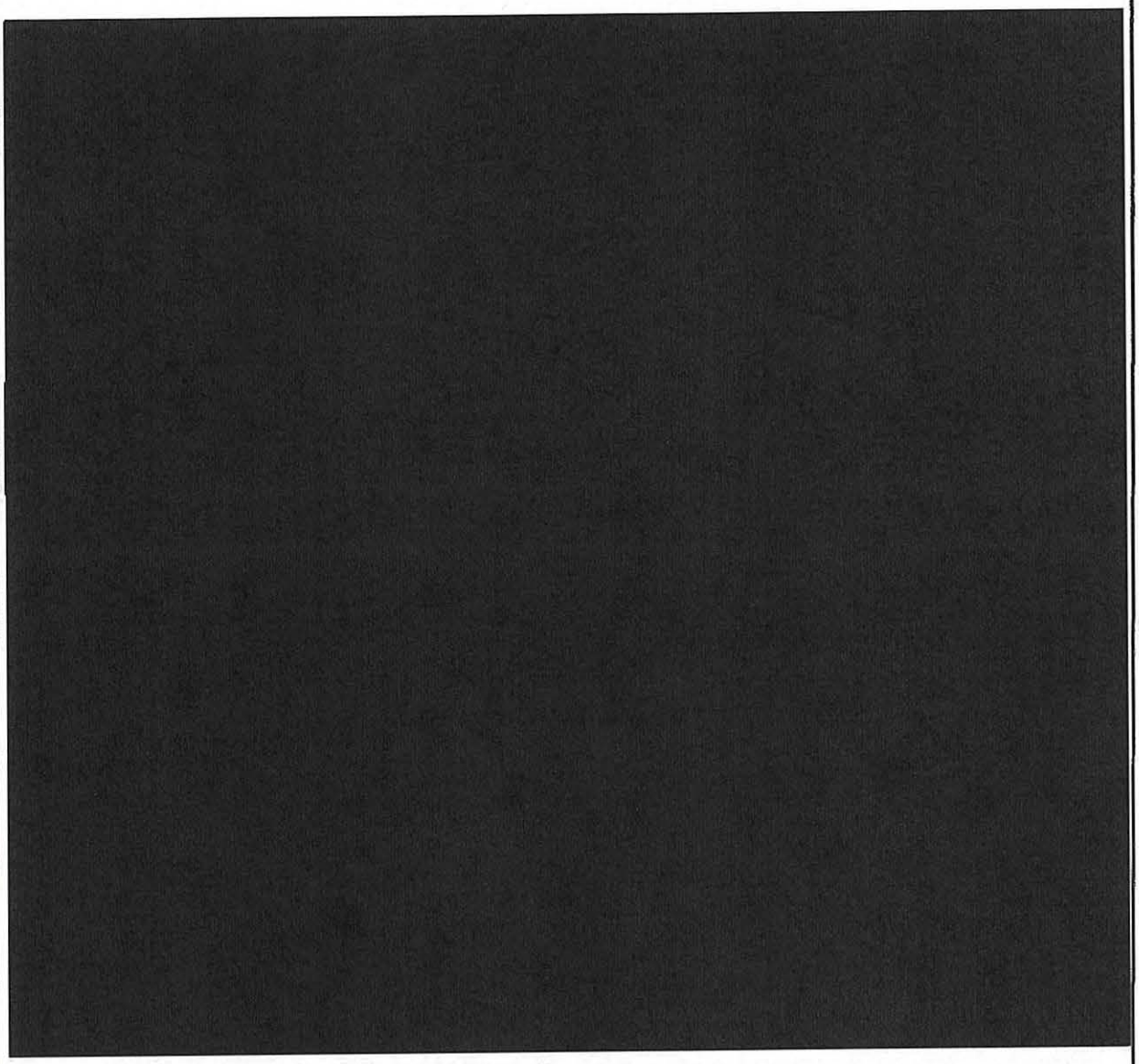
THE COURT: Not too much into the weeds. Apparently, you want to collect non-upstream data under 702 to assist, you said -- [redacted]. What I was curious about was, were there problems or issues that we don't know about that we should?

(b)(6); (b)(7)(C) [redacted] So I'll sort of give you a historical perspective of this, Judge.

So the Court is correct. In [redacted]

[redacted]

[redacted]



THE COURT: All right. Thank you.

(b)(6); (b)(7)(C) [redacted] For the record, I'm noting that they agree.

THE COURT: Everybody is nodding. All right. All right. Thank you. Let me just -- we're going to wrap this up. We have two members of the legal staff here, and if they would like to say anything, they can introduce themselves on the record if they would like to clarify anything that I raised, and they are welcome to do so. Nothing?

THE LAW CLERK: I don't think I have anything, Judge.

THE COURT: I'm going to take under consideration the 702 and approval of the certification and the new targeting minimization procedures.

The criminal case, as I said, can consider the targeting minimization and the certificates for approval, and then we have to consider these by August 27th, and if we need any more information or further information, I'll advise the responsible parties here who are with the staff. I'm generally satisfied that you've met the requirements of the statute. I do want to take a look at a couple of these issues that we've discussed and make sure whether we need any further reporting or other tweaking that's been proposed. We'll take a look at that. I want to thank you all for coming in to work and spending the time today, and I appreciate the work done on these matters, and good to see you all.

(Proceedings adjourned at 12:28 p.m.)

(Certification.)