FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.
SEPTEMBER 7, 2011

[redacted]

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE JOHN D. BATES
JUDGE, UNITED STATES FOREIGN
INTELLIGENCE SURVEILLANCE COURT

APPEARANCES:

DOJ: [redacted]

TASHINA GAUHAR

LISA MONACO

ODNI: [redacted]

NSA: [redacted]

CHRIS INGLIS

[redacted]

P R O C E E D I N G S

THE DEPUTY CLERK: Will everyone please state your names for the record.

[redacted]: [redacted], NSA.

[redacted]: [redacted] NSA Office of General Counsel.

[redacted]: [redacted] NSA Office of General Counsel.

[redacted], NSA.

[redacted], NSA.

[redacted]: Good morning. [redacted] Acting General Counsel, NSA.

MR. INGLIS: Chris Inglis, Deputy Director, NSA.

MS. MONACO: Lisa Monaco, Assistant Attorney General.

MS. GAUHAR: Tashina Gauhar, Deputy Assistant Attorney General.

[redacted], NSD.

[redacted] NSD.

[redacted], ODNI, Office of General Counsel.

THE COURT: Welcome to all of you. Please be seated, and thank you all for coming today. We have a full house, fuller than we usually get in this courtroom.

Now, my view of this proceeding is going to be mainly that I'm going to ask a bunch of questions. I hadn't intended that

anyone give any argument to begin with or opening statement or anything like that. We've been dealing with this issue, the upstream collection and the certifications under 702 for several months, so I don't think there's any need for that.

I'm sure that there will be both lawyers and nonlawyers responding to some of the questions. Since this is a formal hearing on the record, we need to swear, particularly those nonlawyers who will be responding to questions.

It might be easiest if everybody who's going to be responding simply stands up as [redacted] swears those who absolutely need to be sworn. I think that's probably the easiest procedure. So everyone who's going to be speaking and potentially responding to factual issues, please stand be sworn.

(Attendees are sworn.)

THE COURT: All right. So first of all, I want to thank everyone not only for being here but for all the very helpful materials that have been supplied over the past few months. We've looked at them closely, taken them all into account, obviously had questions with respect to certain things, and you've followed up with responses, and all of that is very much appreciated and has advanced this matter considerably.

We wind up at this point with some continuing questions that I thought it would be useful to have you come in and talk with us about, and they are in many areas. By "many areas," I mean they include minimization concerns; they include some

questions about the submissions, looking not all the way back but back one or two submissions; they include definitional questions relating to intent; and they include Fourth Amendment issues. There just are a number of areas.

As I said already, I understand that different people may be responding to those different areas, but let me just jump right in and start with a couple of questions mainly about the August 16 submission, although the questions obviously relate to some of the earlier and the most recent August 30 submission as well.

In the August 16 submission -- I think it's in footnote 5 on page 2 -- the government has discussed and indicated that some of the Internet communications that have been acquired and are continuing to be acquired under section 702 were purged prior to the July 14, 2011, time point in dealing with this statistical assessment and therefore were not included in the NSA sample. I have a few questions about that body of communications that were purged.

Does the government know how many communications were purged and why they were purged?

[redacted]: We do not have an exact account at this point of how many were purged.

THE COURT: Do you have any sense of why they were purged?

[redacted]: There could be a number of reasons:

roamers, overcollect of sorts, and things we would have filed of incidents.

THE COURT: Do we know if any were purged because they were determined to be wholly domestic?

[redacted]: I don't believe any of those were purged because they were wholly domestic.

THE COURT: You don't believe, or you're sure that they weren't?

[redacted]: In our previous filings, we have indicated that prior to our statistical analysis we had not identified any communications of the MCT type that were wholly domestic, which would require purge.

THE COURT: Now, since we don't know much about this purged group -- and this again is just focusing on the statistical sample -- how do we know that the sample is representative of the actual collection of Internet communications? If we don't know what's been purged and what the nature of those purged communications is, doesn't that affect the validity of the sample to the extent that it's a sample of the collection of Internet communications?

[redacted]: The sample that we evaluated were the sample that were in there and available to us.

THE COURT: I understand.

[redacted]: In our evaluation of this sample set, there were some communications that were purged during our evaluation,

but we believe that given the six-month period, the number of items that were included in that six-month period and then the number that we manually evaluated has a statistical representation of that whole body with a 95 percent confidence.

THE COURT: But it seems -- to a fairly ignorant mathematician, it seems that if you're trying to get a representative sample and that representative sample is to be representative of the collected Internet communications but you first take a chunk out of the collected Internet communications, that could affect the validity of that sample.

I don't know how it would affect it or whether it would affect it significantly, but I'm just trying to probe whether it does have some impact mathematically on the validity of that sample as being representative of the collected Internet communications.

[redacted] Your Honor, if I might try to answer that from the General Counsel's Office. We know that the sample that we took was one specific date, and so it's representative a snapshot of time what was in our system.

The reason, Your Honor, that we can't articulate the number of items that had been purged is because we can't put our finger on those in the same way that we can put our finger on what's in our systems at any one point in time. As you may be aware from prior filings, when we discover a compliance incident, it may be several months in time beyond the time that the actual item was

collected.

So that 13.25 million sample that you saw is reflective of what was in our systems as of that particular date. As you march forward in time from the time we took that sample, you would expect that other items that were collected during that time could also be similarly identified through our compliance process and purged.

THE COURT: Well, let me -- this is not intended to be reflective of the truth and is simply for demonstrative purposes, but if you purged 13 million from during that time period, then all the numbers that you're presenting would really only be half of the picture in terms of what's collected.

See, I'm interested ultimately in what's being collected, not what happens to be sitting in your data files at a particular point in time. If the purging that takes place as a normal course of business is half of the material, then it changes everything just from that perspective even without knowing what the purged material is, whether it's of a different nature and richer in terms of wholly domestic communications or not. Just in terms of raw numbers, it would really alter things.

So to the extent that you can tell me something about how much has been purged -- 10 percent, .0001 percent, 50 percent -- it certainly is helpful for me in assessing the impact of the statistical presentation you make.

[redacted]: Right. Your Honor, I think we understand that and appreciate the point. My understanding, though, of the Court's underlying concern was how many of the communications were wholly domestic.

THE COURT: Ultimately, yes.

[redacted]: Right. It has been an unusual occurrence for our folks to find wholly domestic communications in the 702 collections. So, although I can't say it with a certainty, it seems to me that of the communications that would have been purged in the normal course of our compliance regime because either it was a roamer communication or we misidentified a task selector, that those were not likely to have been wholly domestic communications that would have affected the validity of the sample in the sense that we were going through the sample size to actually try to find wholly domestic communications.

THE COURT: I understand that based on your presumptions and the presentation you've made, but even accepting the presentation you've made and assuming that the nature of the purged materials we're talking about right now is the same as the sample you looked at, if the volume of the purged materials is equal to what's left, then the numbers that you've given me have to be doubled.

[redacted] Your Honor, I think it's fair to say that we don't believe that it would be that high, but we haven't come prepared with numbers in terms of --

THE COURT: And you certainly could assess that for the future at some point, because you can look at what's collected and look at what's left during a six-month period, but for now you can't tell me anything more with respect to the six-month period that was analyzed.

[redacted] Those are certainly numbers that we can try to get to Your Honor, but we don't have those today.

THE COURT: Okay. Let's move on.

MR. INGLIS: Your Honor, could we, though, take the action and respond back to you within this week with what we can reconstruct in terms of that purged list?

THE COURT: Yes. I think what we should do is at the end of this discussion decide what you would like to present further and talk about a timeline for it. Let's not do it on one item, because there may be four items by the time we're through.

Staying on the same vein with respect to the August 16 submission, the government states later on in that submission -- I think it's on page 7 -- that NSA cannot determine whether 224 of the roughly 5,000 MCTs examined contained wholly domestic communications. Then a little bit later, it's noted that 23 of the 224 MCTs were not further analyzed because they were subsequently purged or placed on the NSA's master purged list.

With respect to those 23, do we know why those were purged, or are they just part of this broader category that were purged?

[redacted]: Yes, Your Honor. In fact, I believe some of the ones that were purged during the sample time were responsive to the [redacted] incident that was previously reported to the Court in the prior filing. If you recall, I believe NSA purged somewhere upwards of [redacted] total transactions as a result of that [redacted] incident. I can't remember the exact number, but a specific number of that 23 were related to that purge.

THE COURT: Were any of the 23 purged because they were wholly domestic communications?

[redacted]: No, Your Honor.

THE COURT: All right. Then also in the August 16 submission, we have this sort of unknown category which is the -- 45,359 I think is the accurate -- no, I'm sorry. Not the unknown category, but there are 45,359 of the overall sample of 50,440 transactions reviewed that were determined to be single discrete communications. So those were sort of set aside with no further analysis.

In an earlier submission, I think the June 1 submission on page 6, you noted that communications are nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destinations, and certainly that seems obvious to all of us who have dealt with these things.

Because NSA's IP filters [redacted] the government has

indicated that NSA could intercept the communication [redacted]

And then based on a further explanation on pages 7 and 8, I think, of the June 1 submission, should the Court understand that NSA's upstream collection filters wouldn't prevent [redacted]

Do you understand the question?

[redacted]: The filters would not prevent that, and those are examples of the 10 wholly domestic communications that we reference in the August 16 filing. That was exactly the case.

THE COURT: So those communications would all -- those *about* communications would all be subsumed in the category that is identified in the August 16 submission on page 9 as between 996 and 4,965, or would they be in one of these other categories? I don't think they're in that group. Aren't these part of the single discrete communications that you didn't even analyze further?

[redacted]: That's correct, Your Honor.

THE COURT: Aren't there going to be some wholly

domestic communications in that group that you didn't analyze further?

[redacted]: It's possible, Your Honor, but we --

THE COURT: It's more than possible, isn't it? Isn't it likely there will be some *about* communications [redacted], and it's actually a communication that is between two U.S.-located persons?

[redacted]: Your Honor, that is possible. However, typically, [redacted]

THE COURT: How about [redacted]

[redacted]: Yes. It is possible, but the reason why --

THE COURT: It's more than possible. Aren't there going to be a fair number of things?

[redacted]: Correct. There definitely will be. However, the way they're designed is, as I said, [redacted]

[redacted]

THE COURT: The problem that I'm left with is to the extent that there's a statistical presentation to convince the Court of a low volume of wholly domestic communications, this is another category that exists that -- you're using the word "possible," but I have no way to quantify it or know how many in this sample -- just talking about the sample -- knowing how many might be of that category.

[redacted]: Your Honor, I think with respect to the sample that NSA conducted, we certainly endeavored to try to be as responsible as we could in the --

THE COURT: Let me state, you've been very responsible. You've been very helpful. I know you're all doing the best you can. I'm just probing the information.

[redacted]: Certainly. The focus of the sample -- I think you're correct -- was geared towards identifying MCTs within NSA's upstream collection holdings in order to be able to characterize the nature and scope of that collection specifically with respect to multi-communications transactions.

So there may be a number of other things that weren't more specifically looked at within that particular sample which we could attempt to take back and answer for the Court at a later time, but the sample that was run was for the purpose of describing MCTs and the nature and scope of that feature of that collection.

THE COURT: All right. I think it's fair for me to say to you that I am concerned about this category within the sample of 45,000, which is most of the sample. It's by far the majority of the sample and the fact that it does seem to us that there are going to be some *about* communications that are probably wholly domestic communications in that grouping, and I don't have any way to quantify or assess how much it is.

I know you have cautiously, and appropriately, used the term "possible." It seems to me it's more than possible; it is highly likely, but I can't say what it means because I don't know what kind of volume we might be talking about. So let's put that down on the list of something that we may benefit from further information on.

I'm going to allow the legal advisors to follow up with questions on these subjects before I move to another one.

[redacted], FISC legal counsel. Just a follow-up. If someone's [redacted]

[redacted] Do you have a sense one way or another?

[redacted]: It's not necessarily the case that [redacted]

[redacted]

[redacted]: But other than that sort of general observation, you don't have a sense percentage-wise of how many [redacted]

[redacted]: No, we don't.

THE COURT: All right. Staying with the August 16 submission for just a moment longer, the government has concluded -- I think it's on page 9 of that submission -- that of the 13.25 million Internet transactions acquired via the upstream collection during a six-month period, between 48,609, and 70,168 are MCTs containing one or more communications between nontargeted persons but lacking sufficient information for NSA to identify the location of the sender and all intended recipients of that communication.

It's a category that I call "the unknown category," which is fairly large, certainly larger than the category that you've identified as actually containing a wholly domestic communication. A little later in the submission, you indicate that NSA has no basis to believe that any of this category of

transactions contain wholly domestic communications.

Now, that's a fairly absolute statement that's made in the submission. Doesn't the conclusion that between 996 and 4,965, which are pretty low percentages but nonetheless an actual determined amount on this sample, doesn't the conclusion that there are those wholly domestic communications acquired every six months, doesn't that undermine the presumption that none of these unknown transactions contain wholly domestic communications? Wouldn't one expect that at least that percentage of that unknown category would be wholly domestic?

MR. INGLIS: Your Honor, if I might, I'll defer to [redacted] to provide the detailed answer, but in that case, when presented with the possibility that these are either unknown or unknowable, we pushed our analysts further to do two checks against each and every one of these items, first to check to determine whether or not there was any information that might be attributable to a domestic communication, and second, to determine whether there was any information that might lead us to conclude that in fact it was a foreign communication.

In each case, both of those checks for each of these items came back showing that the preponderance of evidence -- not absolutely, but the preponderance of evidence which we had before us would say that there were no domestic communications in that pile.

THE COURT: So I guess what you're saying is that this

grouping, you've determined, is not going to be -- it's going to be less rich in wholly domestic communications than the overall sample is.

[redacted] That's correct.

THE COURT: I mean less rich even to the point of containing no wholly domestic communication. Why is it that this grouping -- what is it about this grouping that should convince me that it is different than the rest of the sample and will contain no wholly domestic communications?

MR. INGLIS: That's more than a fair question. It wasn't that it was wholly devoid of contextual information, that it lacked information, a conclusive statement, but the remaining artifacts led us in every case into a -- if you had to decide yes or no based upon the available information that it was foreign as opposed to domestic. So in each case it wasn't that there was no information. There was insufficient information to say with absolute certainty.

[redacted] Correct. And the way we did that analysis stemmed from the data set we evaluated. Of that 224, we did this in-depth analysis that Chris described, and via a statistical analysis we were able to extrapolate that sample set with a 95 percent certainty across the entire 13 million. And there's a certain error associated with that, and that error is expressed in the confidence interval.

So based on the data set that we evaluated on page 7 and

before, our statistician was able to draw conclusions based on that to the true proportion of those type of communication across the entire 13 million set within that certain confidence interval.

MR. INGLIS: But, Your Honor, if I understand your question, you would ask why do we believe that that population of data that we would declare as unknowable is statistically different than the larger set from which it was extracted, perhaps on a statistically relevant basis.

THE COURT: My guess would be that it goes in the opposite direction because it's a group that has already eliminated all these large portions that clearly don't contain any wholly domestic communications from your view. So why does it then --

MR. INGLIS: In the case of the 10 wholly domestic communications that clearly stood out as having artifacts that said they're wholly domestic. In the case of this pile, there were no artifacts associated with those that spoke to the possibility of domestic that we couldn't rule it absolutely out.

We also looked to see whether in each case there were artifacts that would lead us to conclude that if we had to make a judgment that they were foreign, not domestic, and in which case both of those tests led us to conclude that they were, not presumptively, but more likely, to be foreign than domestic.

There was no information I'm aware of in the file -- and we

pushed our analysts very hard on this particular pile because we had the same question you did, which is could this be a soft underbelly in our analysis, and pushed them very hard, and they came back with no information that would lead them to conclude a strong possibility that they were domestic.

[redacted]: That's correct. [redacted]

[redacted]

THE COURT: Where -- and excuse me for asking the question this way, but I just want all the help I can get. Where should I look in this submission for the explanation that you've given me about the analysis of this unknown group that led you to conclude that it will not contain wholly domestic communications?

[redacted]: It's on page 7 at the bottom.

THE COURT: Page 7 where, sir?

[redacted]: On the second bolder bullet.

THE COURT: Of the 5,081 MCTs?

[redacted]: Yes.

THE COURT: All right. We can read that further and analyze it.

MR. INGLIS: Your Honor, we're happy to be more

responsive based upon what we have and do further analysis as the Court may please.

THE COURT: Well, you can look at it too, and you can mark this down as No. 3. If there's further analysis that you've done that supports the conclusion that you reach that you're now expressing that this unknown category is in fact unlikely, and you think highly unlikely to contain wholly domestic communications, then by all means be prepared to provide it, because on first reading, that's not the conclusion that we reached from assessing this submission.

All right.

[redacted]: Your Honor, just to add into this, I know we haven't gotten into the 30 August --

THE COURT: And I'm not going to be going through it line by line. Don't worry.

[redacted]: But I do think there were at least some portions of the 30 August filing that try to speak to that exact question, and when we get to them, I'll try to --

THE COURT: Okay. Thank you.

All right. Just give me one second to see -- all right. The last question in this area of examining submissions goes back early to the June 1 submission which is clear that the scope of the data that NSA actually acquires through the upstream collection is constantly evolving. And you explained that on pages 24 and 25, noting that [redacted]

[redacted], and all of that can affect the amount and type of data included in a particular transaction.

What I'd like to get a fix on is what this means in terms of any particular sampling at any particular time. In view of that evolution, is it likely that if NSA did a similar analysis, a sampling type analysis of the upstream collection at some later date, two years later than the one done in the recent time period ending in July, is it likely that that analysis would wind up with something significantly or at least somewhat different? This evolution, is it material evolution that really would change things significantly? Or don't you know?

[redacted]: Your Honor, a lot of the analysis focused on identifying MCTs and their percentages showing up in our collection. It is possible that let's say two years down the road that the Internet is more rich with MCTs for a number of different reasons.

We could have [redacted] and that would statistically increase the amount of MCTs.

Because of that unknowable factor of technology popularity in the future, that could change things. Certainly, several years ago, we've talked in the past about [redacted]

[redacted] and as technologies have evolved, that has become more and more popular. So we could see somewhat different results if we were to conduct a similar study in the future. That is definitely something that could happen.

THE COURT: And there's no reason --

[redacted] The other thing I wanted to add, Your Honor, is one of the other factors here that can somewhat limit the evolution is that one of the factors in play here is [redacted]

THE COURT: I think that last explanation of a limiting factor is important because it affects the question I was about to ask, which is, we use the term evolution, and I take it we would look at this with respect to MCTs and say there has been an evolution to the extent that there are more MCTs now than was the case 10 years ago. Correct?

[redacted] I would say that in some cases -- so,

for instance, [redacted] So it's not just so much the MCTs; it's the nature of the MCTs that has evolved as well.

THE COURT: But, in light of the limiting factor that you just mentioned, can we make an assumption that the upstream collection -- let's just focus on that -- will become richer and richer in MCTs, or can we not make that assumption?

[redacted] I don't think we could or couldn't with any degree of competence.

THE COURT: All right. Let's move on to presumptions more generally here. There are several presumptions that the government has urged the Court to continue to rely upon with regard to the upstream collection. They include that [redacted] and that's included in the June 1 submission on page 11.

There's also a presumption that the vast majority of persons outside the U.S. are non-U.S. persons and most of their communications are with other non-U.S. persons located overseas. That's referenced in the June 28 submission on page 5. And there's also a presumption that [redacted] We've talked

about that a little bit, and that's certainly referenced as well in the June 1 submission.

In view of the analysis of the upstream collection that you've done -- and I know we're talking about numbers and percentages here, but in view of that analysis, and in particular the conclusion that the upstream collection does contain a certain number of or percentage of wholly domestic communications over a six-month period as analyzed, can the Court rely on those presumptions as really being absolute, or are they imperfect presumptions at best?

[redacted] Your Honor, if I may, I think they are, like all presumptions, imperfect. I think the numbers we've generated from the study approximate what we expected; that is, a low number of domestic communications when something we think is aberrational is taking place. So we do not intend to say it can never be the case that, but the presumption is it's not the normal behavior, and I think that's what the study bore out.

MR. INGLIS: And, Your Honor, I would add as the chief operating officer of the National Security Agency and having to then essentially sign up to our end of a representation, that I feel the same, that the preponderance of those assumptions has been borne out by the data to be correct but imperfect and that what we then have to apply are a set of procedures to ensure that we are looking for those exceptions and that we act appropriately when we discover those exceptions and that we can

therefore offer back that the totality of that has a high probability, again not absolute, but a high probability of making the right call in terms of what our presumption should be and having a high probability of catching the exceptions that then ensue and dealing with those appropriately.

THE COURT: Let's just turn back the page a moment to something we were talking about a minute ago with the evolution of the Internet. Any sense of what, for example, [redacted] might do to these issues and the way that Internet communications are routed?

[redacted]

So at this point, we haven't seen any change, and I'm not too sure what we would expect to see just given the nature of [redacted].

THE COURT: We're talking about imperfect presumptions. To the extent that NSA is acquiring [redacted] should the presumptions be reversed? In other words, should we instead presume that communications are within

the United States and with U.S. persons?

MR. INGLIS: Your Honor, I think that question centers on [redacted], so I would ask [redacted] to talk to that.

[redacted] Just to clarify, the question is, is should we presume at some future date that a U.S. service provider is primarily servicing U.S. persons? Or...

THE COURT: It's a little less than that. It's just if the acquisition is [redacted] of someone in the United States, do the presumptions that you rely on and urge the Court to apply hold up, or should we actually think that the opposite would be true, that for those acquisitions, the presumptions, if you're going to apply a presumption, the presumption should be that the communications are within the United States and with U.S. persons?

[redacted]: So if the person was in the United States and [redacted] and we intercepted that, would we presume at some future date that that was -- I'm not sure I fully understand.

[redacted] If I can address it, Your Honor. I think that that would be an excellent presumption to reverse if not for the presence of the targeted selectors. So remember that the reason that we collect any particular transmission is that it contained the target selector which would be an independent determination that the target is reasonably to be

outside the U.S. So that weakens otherwise what I think would be the natural inclination to reverse that presumption.

[redacted]: If you've got a transaction that is [redacted]

[redacted] With respect to those individual discrete communications, what presumption, if any, should be applied?

[redacted] In that scenario that you've described, if [redacted], we still are applying the IP filtering process. So if that user was [redacted] So that particular scenario wouldn't occur. [redacted]

[redacted] So that is what happened in the 10 examples we have. [redacted] We think we're going to very, very rarely see that happen because the overall presumption of the statute, remember, is that the whole world out there is using the services here.

[redacted]

[redacted]

That's the scenario -- and we've seen it play out in this study on 10 occasions -- that's a scenario that you're raising. But it won't be somebody in the United States communicating with [redacted] in the United States.

[redacted]: Just to make sure the point is crystal clear for the Court, the concern that the Court has about what presumption to apply to communications [redacted]

[redacted] which was the exception in the study, not the rule. Is that a fair statement?

[redacted] That's correct.

MR. [redacted]: And I think it's also important to remember that the presumptions aren't the first resort. The presumptions are in many senses a last resort. There can be objective indicia of the location of the communicants that is more reliable than the presumption. The presumptions apply

ostensibly in the absence of information to the contrary, and implicit in that requirement is a due diligence requirement to actually try to assess whether there's any objective information that to the extent you need to rely on the presumption that would rebut the presumption.

I think NSA's manual review bears out that the digging can result in the location of reliable, objective information that is indicative of a person's location.

MS. MONACO: Just to press on that one bit, I think that's why the Court is struggling with the 224. NSA only arrived at that 224 because the NSA works through all of the objective indicia that [redacted] mentions, and then, only then, after discarding all of that and identifying all of that and making conclusions from it results in the 224 where there were no reliable indicia.

THE COURT: To round this out -- and [redacted], if you have more questions, please feel free to ask them -- but let's talk about the [redacted] situation for a moment that I already referred to. [redacted]

[redacted]

[redacted]: [redacted]

[redacted]

THE COURT: [redacted]

[redacted]

[redacted]:

[redacted]

THE COURT: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THE COURT: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THE COURT: [redacted]

[redacted]: [redacted]

[redacted]

[redacted]

[redacted]

THE COURT: [redacted]

[redacted]

[redacted]: [redacted]

[redacted]

THE COURT: [redacted]

[redacted]

[redacted]: [redacted]

[redacted]

[redacted]

THE COURT: All right. Okay. Let's move on to the question of intent. This is sort of a difficult question to answer. It's an easy question to ask, but I'll throw it out there, and I can be more specific if you'd like me to be.

The government's submissions do use various terms -- intentional, unintentional, inadvertent, incidental -- when describing the upstream collection or aspects of the upstream collection. I'm a little confused as to what is meant, and rather than just throwing that out to you, let me ask one or two specific questions.

Is unintentional the same as inadvertent? As you use those terms, are they the same? Do both mean "not intended?"

[redacted]: Your Honor, I think that's correct. "Inadvertent" is a term that's used in the NSA immunization procedures, and "unintentional" has been used in various documents as well. But I think "inadvertent" and "unintentional" can mean the same thing.

THE COURT: And "intentional" is the opposite of both "unintentional" and "inadvertent."

[redacted]: Yes.

THE COURT: And "incidental" means what?

[redacted]: "Incidental," I think as we've framed it, means something that results as a consequence of an action that

we take intentionally.

THE COURT: Is happening or a byproduct --

[redacted] It's not our intent in taking that action, but as you said, it's a byproduct of that action. So in an MCT, for example, our intent is to acquire a communication to, from, or about a targeted selector. At the time we acquire that transaction, we may not even know that it's an MCT that contains other communications.

So we acquire the MCT because we see, hey, that's a communication that has a targeted selector. We reasonably believe that that has foreign intelligence information in it. We acquire it, it's turns out it's MCT, it's got other communications in it. We still intended to acquire that transaction and anything contained within it such that to the extent there are these other communications in it, it's incidental to our acquisition of the transaction.

THE COURT: All right. Let's drill down a little more. The June 28 submission states that "acquisition of Internet transactions is intentional," and on the same page, page 6, further states that "given the government's knowledge that such transactions may also include information that is not to, from, or about a task selector, the acquisition of this additional information is not inadvertent."

[redacted] I think that's correct.

THE COURT: Later in the same filing, and also in the

August 30 filing, the government seems to be saying that any wholly domestic communication that is acquired as part of a transaction is obtained unintentionally or inadvertently. Is that also correct?

[redacted]: Yes.

THE COURT: Now, NSA knows with certainty that both will be acquired. In other words, wholly domestic discrete communications are simply a subset of the nontarget discrete communications that you acquire as part of a transaction. So how do you reconcile that with these statements with respect to intentional or unintentional?

[redacted]: So we intentionally acquire MCTs because they contain the presence of a targeted selector that we believe is used by a non-U.S. person located outside the United States. However, we don't intentionally acquire all such MCTs. We know that we cannot acquire --

THE COURT: You knowingly acquire them, though.

[redacted]: But we don't intentionally acquire them.

THE COURT: Well, we'll get to that in a moment.

[redacted]: Understood. And we may not know at the time of acquisition that that MCT is something that contains --

THE COURT: With respect to a particular transaction.

[redacted]: Exactly. So we are intentionally acquiring MCTs, but we have also implemented [redacted] means to ensure that we are not intentionally acquiring wholly domestic

communications, but we believe that those [redacted] means are reasonably designed to prevent that. Granted, they are not perfect, but we do believe that they are reasonably designed to prevent the acquisition of those communications.

THE COURT: Let's jump to the statute for a second. Under section 1881(a)(1), the Court is required to determine whether the targeting procedures are, in the language of the statute, "reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."

Let's look at those two parts of that statutory provision. Intentional acquisition.

In the government's view, what's the meaning of "intentional" as used in the statute? And to set the framework for you, I think in criminal law and in tort law it's generally settled that a person intends to produce a consequence either when he acts with a purpose of producing the consequence, which is what you've been focusing on I think in your papers and here for the moment, or, when he acts knowing that the consequence is substantially certain to occur.

It does seem to me that you really focus on the first part of that traditional definition, because you're really only talking about the specific-purpose definition and not the knowledge of substantial certainty aspect of intent. Am I

right?

[redacted]: I think we need to focus on the fact that -- I mean, granted, the statute says that we are precluded from acquiring communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States. I grant you that we may not have focused specifically on that aspect, our knowledge at the time of acquisition. I think NSA's manual review has shown that it can take a lot of drilling down into these communications to determine whether or not they are in fact wholly domestic.

THE COURT: Well, it doesn't take that much drilling anymore to determine that there are some that are wholly domestic. It does take a lot of drilling, if you even can, to determine that a particular transaction is wholly domestic or a communication within a transaction is wholly domestic.

Indeed, it's especially true or especially difficult when acquired, but it doesn't take much now to conclude, because that's what your analysis has concluded, that there will be wholly domestic communications acquired. Certainly will be.

[redacted]: No, no. I agree a hundred percent with that, Your Honor. But again, at the time of acquisition, we may not know it, and it's at the time of acquisition that the statute precludes us from intentionally acquiring a domestic communication.

THE COURT: Then we're getting a little bit semantic.

It depends on what you mean by "acquisition," whether you mean acquisition of a particular communication, acquisition of a particular transaction, or the acquisition that takes place during the space of a day, or an hour. If it's either of the latter two, you know that there's some wholly domestic communications that are being acquired, statistically.

[redacted]: Statistically, yes. Personally, the way that I've always viewed the way that that provision in the statute works is it's on an acquisition-by-acquisition basis, and "acquisition" meaning communication-by-communication basis, because we are targeting to acquire foreign intelligence information. That foreign intelligence information is contained in individual communications.

THE COURT: Do you think that definitionally, the Court, when it's interpreting and applying 1881(a) in this setting, should only be focused on the purpose portion of the definition that I went through a moment ago, or should the Court also be looking at the knowing aspect of it -- in other words, that part of the definition of "intention" at to be applied here is "not only acting with a purpose of producing the consequence but also acting knowing that the consequence is substantially certain to occur"?

Should I be jettisoning that portion of the traditional "intentional" definition and applying some narrower definition here? Or are you only saying that even applying both prongs of

that definition you need to look at what's happening and what's known at the time of the acquisition of a specific transaction?

[redacted]: I think it's the latter, and I also think that the fact that the statute says that the procedures have to be reasonably designed to prevent the acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.

I think given that language, the statute contemplates that there's not going to be a perfect system. It has to be a reasonably designed system, and I think the results of NSA's manual review bear out the fact that the system that NSA has designed, albeit not perfect, is reasonably designed to prevent the acquisition that the statute prohibits.

[redacted]: Your Honor, if I could add one thing. If we could take away some of the complication of this discussion by focusing just on other than MCT, for what it's worth, I think the Court has already considered and countenanced the idea that some targets are going to roam into the United States, or we could turn out to be wrong and they would be in the United States. And some statistically, probably a very small percentage of those may have communications with other people in the United States.

So, to a certain extent, this may be a threshold the Court has already crossed or at least walked up to and assessed. So I

would just like the offer that in the context of this question about what the statute means.

THE COURT: I think that's a fair point in terms of we all know that systems are not going to be perfect. We've already faced some instances, and this may be another one that is an acceptable imperfection. But that's what we have to explore a little bit more before the Court is prepared to reach that conclusion.

We've already talked a little bit about the second part of the statutory term of the "known at the time of acquisition." So it would be your view that the knowledge or the certainty that the collection will result in the acquisition of thousands over the course of a year of wholly domestic communications does not mean that there's a violation of 1881. Set aside the "reasonably designed" language, which I think is important, but just set that aside for a second.

[redacted]: I'm not sure I understand the question.

THE COURT: Well, you know at the time of acquisition that there are thousands of transactions that are going to be wholly domestic over the course of a year. At the time of acquisition of a particular transaction, you don't know that that transaction is wholly domestic.

Your assessment is that even on this knowledge prong of the definition and looking at the "known at the time of acquisition" language of the statute, that the Court should really not be

troubled by the fact that it's known that there are going to be thousands of wholly domestic communications acquired -- and again, I'm only focusing within the statutory language now; I'm not talking about the Fourth Amendment -- shouldn't be troubled by that because it's not known that any particular transaction is wholly domestic and that the Court therefore need not be troubled by the fact that everyone knows that there will be some wholly domestic communications acquired.

[redacted]: It's certainly reasonable to presume that we are going to be acquiring wholly domestic communications despite our best efforts, and that's why, as we've shown in the papers, we're relying heavily on the application of our minimization procedures.

So to the extent that the protections that we put into place at the time of acquisition don't work, then we have these substantial back-end protections to ensure that to the extent that one of these domestic communications resides in an NSA system because it couldn't be weeded out at the point of acquisition, and an analyst comes across it during the course of their regular analytical work, that that information is treated appropriately; i.e., we've committed to destroying any wholly domestic communications or MCTs containing even a single wholly domestic communication. So I think the two in tandem work together.

THE COURT: I have one or two more questions in this

intent section, if you will, and then I think it'll be -- well, let me not assume that we won't have a few more than one or two questions. Some of this relates to Judge McLaughlin's 2008 opinion, because you do rely on it to a certain extent, back in the June 28 submission, for example.

You rely on it for the proposition that NSA's acquisition of transactions continue discrete communications that are not to, from, or about a task selector is intentional because the acquisition of the additional information is a necessary yet unavoidable consequence of acquiring foreign communications to, from, or about a task selector.

Judge McLaughlin, in that opinion, also found that a communication would be unintentionally acquired for purposes of 1806, if, for example, the acquisition resulted from a technical malfunction or an inadvertent misidentification of a selector.

Is the government's argument that its acquisition of wholly domestic communications is unintentional based on NSA's determination that its filters are not functioning properly, or is it instead that the filters have a limited capacity to prevent the acquisition of wholly domestic communications?

[redacted]: I think it's both. I think we've previously asserted that to the extent that NSA's filters fail for a technical reason -- and that has happened in the past, and we have reported a compliance incident related to that, and we acquired wholly domestic communications as a result of that --

that is a situation where we've unintentionally acquired a wholly domestic communication. In this instance, it's not --

THE COURT: It's not a failure. Isn't it more a limited capacity?

[redacted]: It's a very small limited capacity. But, yeah, I think it's pretty much --

MR. INGLIS: But, Your Honor, I would offer and add that I think it's more the limited capacity, the limited technical possibility given the way the communications work, that if we had the means to devise it such that it would screen out at that moment in time -- discern, screen out -- we should be expected and would do so.

THE COURT: If it's that limited capacity or feasibility, why isn't the acquisition of those communications, to return to Judge McLaughlin's language, a necessary yet unavoidable consequence of acquiring communications to, from, or about a task selector and therefore intentional, under her opinion?

[redacted] Under her opinion, and as we argued to the Court, we were basing our assertion that there were certain types of communications that were intentionally but mistakenly acquired based on our understanding of where the target was also. That's where our primary focus was.

This situation is a little bit different than that. In that instance, we were relying wholly on our reasonable but

mistaken belief that our target was located outside the United States in assessing whether or not, to the extent that that person roams into the United States, 1806(i) applies in that case.

We determined that it didn't because we were at all times intending to acquire all communications from our targeted selector under the reasonable but mistaken belief that our target was located outside the United States.

In this context, it's a little bit different. Rather than relying on the application of the targeting procedures and relying on our reasonable belief, we are taking active technical measures to prevent the acquisition of wholly domestic communication. That's the distinction that I draw, and when those technical means don't necessarily work, that's when the acquisition becomes unintentional.

THE COURT: All right. So if we have an acquisition of wholly domestic communications in a circumstance where [redacted] okay, so that's the situation -- would the acquisition of those transactions by the upstream collection be intentional?

[redacted]: I just want to make sure we understand the question.

THE COURT: I'm talking about acquiring wholly domestic communications in circumstances where [redacted]. In that situation, wouldn't acquisition through upstream collection be intentional, even though it's based on a mistaken belief that the target was outside the United States?

[redacted]: I would argue that it's still intentional, because recall that the IP filtering and [redacted] is intended to prevent the acquisition of wholly domestic *about* communications. In targeting procedures, we rely on the presence of the target to ensure that we're not acquiring any wholly domestic communications.

The fact that in practice we apply the IP filters and [redacted] to all communications, including those of the target, I think doesn't undermine the notion that we've relied on in the past that to the extent that a person believed to be located outside the United States roams into the United States and we continue acquiring their communications, albeit some of which may be domestic, that that is still intentional but unknowing.

THE COURT: All right. [redacted], in particular, did you want to ask anything about the -- I guess it relates back to the [redacted] of the collection?

[redacted] Sure. So, back in 2009, the government reported an overcollection [redacted] overcollection incident.

Immediately following that overcollection, the government took it upon itself to purge the overcollected communications from NSA systems in order to ensure that no information had been disseminated by NSA in any form and to deploy improved filtering systems to prevent the future acquisition of such nontarget communications.

In Judge McLaughlin's opinion in improving that surveillance following the [redacted] overcollection incident, she relied heavily on those remedial and preventative measures in concluding that the overcollection didn't preclude the approval of the certification and the procedures before her for renewal.

The approach being followed here seems quite different in that the NSA's proposing to continue collecting nontarget information as part of Internet transactions and to keep and potentially use much of that information. So can you address the difference in why you're treating them differently?

[redacted]: I think the key difference is in the [redacted] incident, the overcollection resulted in the acquisition of

[redacted]

Here, we are only acquiring transactions because they contain a targeted selector. At the time of acquisition, we may not even know that there are other discrete communications within the transaction that aren't to, from, or about the targeted selector. I think that's a very key difference.

Also, another important difference between [redacted] and this situation is, in [redacted], there was a technological fix that could be implemented. The [redacted] was preventable, and NSA did a lot of great work in developing technical means to ensure that those types of overcollections don't happen again.

Again, those means aren't perfect and every once in a while something slips though, but by and large, those are technical means that NSA has implemented to prevent the sort of overcollection that occurred in [redacted] Those technical means aren't available here. NSA lacks the technical means to prevent -- or can only acquire whole transactions. They can't unpack, generally speaking, transactions into their component discrete communications [redacted] So I think that's another key difference.

So, just to sum up, it's the nature of the overcollection. In [redacted] there was no nexus to the targeted selector at all, whereas here there is a nexus to the targeted selector that results in the acquisition, presence of the targeted selector in the transaction, and in [redacted] there was a technical fix that could prevent what was overcollection. Here, there's not a technical fix that will enable NSA to conduct the acquisition in a more discrete way.

THE COURT: All right. Let's talk about that for a second. Is it clear from your submissions and your assessment of your technology that NSA doesn't currently have or employ technology that would permit it to acquire everything it's authorized to acquire without also acquiring MCTs?

[redacted]: That's correct.

THE COURT: Is it technically possible -- in other words, within your knowledge of technology, is it technically possible to come up with a means to acquire everything but not MCTs? I know you don't have it right now, but I'm trying to examine whether it's possible.

[redacted]: There's sort of two components to that. One is that these technologies are not designed to do that by nature, and as a result, it is very technologically difficult to do that in many cases. Some cases it is impossible, but in terms of us being able to -- let's use [redacted] as an example. Could we develop a technology which could [redacted]

[redacted]

However, the viability of that [redacted] would be very short-lived, largely because [redacted]. [redacted].

Compound that by [redacted], it becomes a very hard and infeasible task to do, especially considering that NSA is only looking at [redacted]

[redacted]

THE COURT: Have you already looked at this issue and made sort of the final determination by NSA that there isn't a means to come up with a technological, as [redacted] put it, fix?

[redacted]: Yes. We have concluded that it's technologically infeasible to do this.

MR. INGLIS: I would go further to say that if [redacted]

[redacted]

It will necessarily change, and we therefore will always design

imperfect systems against tomorrow's probabilities.

THE COURT: But not to be glib, that's your business, isn't it? Isn't that what you do every day in all of these multitude of settings?

MR. INGLIS: That's exactly right, sir, and fairly put. I would say that we cannot perfectly anticipate those changes. So the machinery will fail before we detect it, and then upon detection, we will have to then correct it.

MS. MONACO: I might add if I could, Your Honor, in our discussions on this issue preceding this hearing, we also discussed the fact that some of this relies on [redacted] if that's a fair statement for my colleagues.

THE COURT: All right. Let's talk about minimization for a second. More than a second. In the most recent submission, NSA has indicated that it will require any analyst who wants to use a discrete communication within an MCT to first perform checks to determine the locations of the users of electronic communications or accounts or addresses, identifiers referenced in that discrete communication "to the extent reasonably necessary" to determine whether that communication is wholly domestic.

If the analyst determines that the active user is a task

selector or is located outside the United States, then no further checks would be done. If the active user is not a tasked selector or is not determined to be located outside the United States, what happens?

[redacted]: If the active user is determined to be not in the United States?

THE COURT: I think the way I'd actually say it is the active user is not a tasked selector or is not determined to be located outside the United States, what do you do then? Can the analyst use the communication, or are there additional checks that are necessary?

[redacted]: There were additional checks. In that case I think there were [redacted] of those that were identified in that filing, and for each of those the analyst went into deeper technical analysis of all those discrete communications and determined that those discrete communications were not wholly domestic.

[redacted]: But how can you describe the further checks?

[redacted]: They went into the content and verified that all of the [redacted] contained at least one foreign recipient.

THE COURT: That was done in the context of the sampling, you mean?

[redacted]: That was done in the evaluation of the case

where the active user was located within the United States.

THE COURT: Is that what an analyst is going to do tomorrow when they have this circumstance?

[redacted]: If they were going to use that data, that's what they would do. That's correct.

THE COURT: And if the analyst is unable to determine that at least one of the communications is outside of the United States, what happens then?

[redacted]: If it was inconclusive, it would be likely that they would not use that piece of data.

THE COURT: Is that what the protocols and policies require? Can the analyst use the communication, or is the default, if you will, that he or she has to treat it as a wholly domestic communication?

(Pause)

If you need a second to consult, by all means take it. There's no harm to doing that. You're free to do so.

[redacted]: Thank you, Your Honor.

(Attendees conferring.)

[redacted]: Unless we could confirm, we would not use that piece of data.

THE COURT: So that would be the default position.

Just for a second, you referred to these [redacted] checks, and my question is really whether those are going to be used going forward, and where do we find in the submissions that you've

indicated that those are going to be used going forward?

MR. INGLIS: Your Honor, I think the answer to your first question is yes, the checks that we have imposed will go forward, and as to where they are documented at that level of detail, we'll determine.

[redacted]: Your Honor, I think you're referring to things that are detailed on page 8 and 9 of the 30 August submission which details the very steps that NSA would take.

THE COURT: 8 and 9?

[redacted]: Yes, Your Honor.

THE COURT: Okay.

[redacted]: Your Honor, we may be mixing things.

THE COURT: Talking past each other or apples and oranges?

[redacted]: If you look at the August 30 submission, the first clarification that the government makes is one regarding wholly domestic communications and if an analyst who is confronted with an MCT wants to make use of some discrete communication within it, they will first do the checks that we've just been talking about to determine whether or not that communication is wholly domestic.

And I don't know that we got into it at this level of detail, but if you look at page 3, we do there talk about what the analyst will do in order to aid the analyst in attempting to recognize whether or not they are in fact dealing with a wholly

domestic communication.

THE COURT: All right. And we can refer back to those. Thanks.

All right. Now, in the August 30 submission, another point made -- I think it's on page 9 -- is the government indicates that if NSA acquires, through this upstream collection, a discrete communication that is not to, from, or about a tasked selector but is to or from an identifiable U.S. person, that communication cannot be used for any purpose other than to protect against an immediate threat to human life.

Who's going to make that determination? An analyst? Or is there a process for how that determination is made and who makes that determination?

[redacted]: Your Honor, is the determination you're talking about whether or not the specific item could be used or whether or not the U.S. person could be identified?

THE COURT: Whether it can be used.

MR. INGLIS: It could only be used to protect the life of a person. We have a defined process at National Security Agency in which we involve our general counsel in in order to make that determination.

[redacted]: And, Your Honor, if I may, that language is similar to language that appears in NSA's minimization procedures at the very beginning, basically a threat-to-life carve-out. But like that threat-to-life carve-out and the

minimization procedures, there's complete transparency on the part of the government because if NSA needs to take that action, they need to report that to DOJ and ODNI, and we in turn have to report that to the Court.

THE COURT: I understand that. I'm still interested in how that determination is made. The fact that it's reported to the Court later on that a determination was made and it was used is important, but it's also important to know that there's an appropriate process for making that determination within NSA.

Now, if there's no immediate threat to human life in that same circumstance, does NSA retain the communication?

[redacted]: We would, Your Honor.

THE COURT: And is it marked in some way to indicate that it cannot be used without that determination being made, or is it just there?

MR. INGLIS: Your Honor, I do not believe we marked that communication at that moment in time.

THE COURT: Do you think there's a need to, or do you think an analyst in the future, when confronted with this communication and making a decision on whether to use it, will be sufficiently apprised of the fact that it's a wholly domestic communication and that he or she needs to follow this process in terms of a threat to human life?

[redacted]: It wouldn't be a wholly domestic communication.

THE COURT: I'm sorry. It's not a wholly domestic communication. You're right.

[redacted]: I think that it's pretty clear that it would be better if it were marked than not marked if the government knows about it. The feasibility of doing that I don't think we've assessed, so I don't think we can commit sitting at the table to do that. But we will seriously consider whether it's possible to do that, or when we review it, if it's tentatively possible.

MR. INGLIS: And so in the absence of that marking the confidence that is placed upon common-training standard that the analyst had, the fact that if it were determined to be wholly domestic a further check that it would be purged in all of its derivatives as well.

THE COURT: Let's move from the specific to the more general. Is it possible for NSA to segregate the upstream collection from the rest of its 702 collection?

[redacted]: It's possible.

[redacted]: The upstream collection in comparison to our PRISM collection, as we've referred to it, they are commingled in the database, but they are marked in such a way such that they can be identified from distinguishing sources.

THE COURT: So in a sense, it is separated by being marked. It's all commingled in the same database. Is that commingling in the same database just as good as a complete

separation in terms of the use of tools to pull out the communications that can easily be identified as to, from, or about a task selector? In other words -- well, I think the question is a little confusing.

MR. INGLIS: Is your question, Your Honor, whether it can be better or worse depending upon how you choose to organize the data?

THE COURT: If you separate it rather than commingled and marked, would it be easier to deal with the concerns that exist with respect to a portion of the upstream collection technologically?

[redacted]: I don't think that the commingling is a factor in determining and marking the data for the analyst to know that this is from upstream versus not upstream or that there is an MCT involved or not. I don't think that the commingling is a factor of that.

MR. INGLIS: So, Your Honor, not to extend the conversation into an inappropriate corner of little interest to the Court, but NSA's strategy writ large for its technical architecture is in the face of increased commingling to concentrate on the marketing of such data element such that we can then determine its provenance.

Increasingly, what we'll have is many variables with respect to the origins, the policies that pertain to data and many variables with respect to the authorities and privileges of

individuals, and as that M meets N, the prospect of coming up with M times N, different instantiations of data sets that are physically separate, that's infeasible for us. So our strategy is to go towards the marking and to allow commingling to happen, not sloppily, but there's no real other tenable design.

THE COURT: I have a couple more questions on minimize, but go ahead.

[redacted]: If I could just follow up on that. I guess what we're trying to get at here is whether it was technologically feasible to separate this data out given that there are concerns about what's in it -- wholly domestic communications, lots of U.S.-person information, nontarget U.S. person information -- whether you physically separate it or separate it via marking rules, access rules.

Is it possible to segregate that, such that you could then limit access to it? I guess one of our concerns is, as I understand it, it comes in to your database and pretty much immediately is made available to analysts running queries. So if something is responsive to a query, it will come up and they will see it.

We were curious as to whether it would be technologically possible to sort of either segregate it and sort of immediately or soon thereafter pull out the stuff that you know is okay and make that available, or, alternatively, or perhaps in addition, limit the access of the stuff that's problematic to people who

are specially trained or subject to certain additional access.

MR. INGLIS: If I may, I think I hear two questions, but correct me if I got that wrong. The first is can there be, upon the collection and the immediate presentation of that collection to either machine or a person, some distinguishing characteristic, either some physical segregation or some mark that goes along with that, atomically bound to that, such that there's no doubt where this came from. It's either upstream, or it's all other. I think the answer to that question is yes.

THE COURT: If you can mark it, presumably you can segregate it.

MR. INGLIS: Yes. But I think the further implied question is, is there then some meaningful processing that might occur so that you can then winnow and filter that material before presentation, before some manual application procedures, and we don't yet know of those. We have thought hard about that, and we don't yet know what further processing might occur absent introducing the human into the loop and having that human follow a rule set that would help determine what the further provenance or not of that data might be.

[redacted]: But you have the capability to put the human in the loop. You have this specially trained cadre of analysts who are working with your manual database. Theoretically, you could have a specially trained cadre --

MR. INGLIS: So given the answer to the first

question, is it possible to alert the human beings that come into contact with that data that there are certain rules that pertain that you must handle this data, ask questions of this data in a certain way.

MS. MONACO: As the Court sees from the August 30 submission, that's exactly what the proposal is to do going forward, to apply a banner to this collection so that would effectuate the alert Deputy Director Inglis talked about, and also that coupled with the training and guidance for the analyst working in concert would apply the protections to that potentially problematic material.

THE COURT: Let's go on to another minimization area. Under section 3(b)(1) of the NSA minimization procedures, "NSA personnel will destroy inadvertently acquired communications of or concerning a United States person at the earliest practical point in the processing cycle at which the communication can be identified either as clearly not relevant to the authorized purpose of the acquisition or as not containing evidence of a crime," and that's all in quotation marks.

But in the June 1 submission, I think at page 22, it's indicated that NSA cannot destroy a discrete communication within an MCT without destabilizing and potentially rendering unusable some or all of the collected transaction including the single discrete communication which is to, from, or about the task selector.

So, assuming the communication of or concerning a U.S. person is not a wholly domestic communication, would NSA retain the entire MCT for five years regardless of that destruction requirement in section 3(b)(1)?

[redacted]: That's correct, yes.

THE COURT: And would the communication of or concerning a U.S. person be available to NSA analysts during the entire five-year period?

[redacted]: So again, Your Honor, I think this goes back to an earlier question you asked, which is would we mark it once we discover that's true. I think that's a valuable thing to do and to look into. For reasons already described by [redacted] we couldn't eliminate that piece of the communication without eliminating the whole communication.

So the line we're proposing here is, if we find a domestic communication within the series of communications, we'll destroy the whole transaction. If we find untargeted person information, we won't destroy, but we won't use that either.

THE COURT: Now, these communications will start unminimized and eventually be minimized. Does NSA share unminimized MCTs acquired through the upstream collection with any other agencies? CIA? FBI?

[redacted]: No. At this time the only collection that's shared with the CIA or FBI is from the PRISM side, [redacted]

THE COURT: So the upstream collection is not shared at all.

[redacted]: Correct.

THE COURT: Except on an individual basis once an analyst has focused in on a particular --

[redacted]: Not shared wholesale. That's correct.

THE COURT: How about with foreign governments for translation purposes or analytical purposes under section 7(b) of your minimization procedures?

[redacted]: [redacted]

THE COURT: So just to close out the minimization, unless any of the legal advisors have questions, the manual review process is not going to be continued prospectively. Correct? In other words, NSA proposes to rely on analysts who recognize wholly domestic communications within transactions when they're confronted with them.

MR. INGLIS: Sir, by the manual of due process, you mean the process by which we examined the slice of 50,000?

THE COURT: Yes.

MR. INGLIS: We don't intend to carry that forward. We intend to carry the training standard forward for the analysts who encounter the data.

THE COURT: So wholly domestic communications that are never viewed by analysts will remain in the repositories for

five years.

[redacted]: That's correct.

THE COURT: And with transactions that are reviewed, should the Court be confident that NSA analysts would be able to recognize wholly domestic communications when confronted with them in their daily work? There's been -- even in this sampling process, there's been some difficulty in recognizing wholly domestic communications.

Should we be confident that analysts will be able to do that? Presumably, they're going to have less in the nature of tools, time, and resources than were employed during this analytical exercise.

[redacted]: Your Honor, I think the Court should be confident, and really for a couple of reasons. First off, the 10 domestic communications that were confirmed during the review of the sample were all communications that when you actually looked at them they were not responsive to any foreign intelligence requirement whatsoever, so it was unlikely that in the normal course of business our analyst would have pulled them up in the first instance. Therefore, by operation of NSA's minimization procedures just sort of by standard, they would have aged off in five years.

But secondly, the amount of training, the notices to the workforce, the related efforts to be sure that the workforce is aware of the problem I think will sensitize our analysts to be

on the lookout for the possibility that an MCT that was responsive to a query they made of a database might be a wholly domestic communication and therefore they should go through the steps that we've outlined in the filings to make sure that they've properly accounted for it and made sure that it is not in fact a wholly domestic communication.

MR. INGLIS: Your Honor, if I might add, they're not advised to go through those checks; they're compelled to go through those checks. What we found as a practical matter in this particular activity where we manually examined the 50,000-plus transactions is part of the difficulty in having analysts identify wholly domestic communications is that they were not in practice in terms of finding any meaning or use in them.

So we actually had to have them pursue matters that more often than not they would say that is of no interest to me; I wouldn't pursue that naturally. And so then becoming comfortable with the artifacts that are associated with wholly domestic communications that are otherwise uninteresting and otherwise not things that they would daily work with was in fact in my view an opportunity to understand why they then would necessarily go after those things that are directly responsive to their queries, as opposed to those things that were incidentally collected.

THE COURT: Now, I have one more of area of questioning that's really under the umbrella of the Fourth

Amendment and probably 15 minutes maybe at most, but there may be other things that we'll need to discuss and other things that you may want to say.

In asking this question I'm concerned about all of you, but I'm most concerned about [redacted] the court reporter, and that is whether we should take a short break now and resume in five to 10 minutes, probably for another -- it depends how much you would to say after I finish with the questions.

The questions themselves probably won't take more than 15, at most 20 minutes, but I don't know what further we might need to discuss from your perspective. Anyone think it would be advantageous to take a short break?

MS. MONACO: Well, Your Honor, I don't want to impose on [redacted] --

THE COURT: I'll ask him independently. He may answer that question yes, and that'll be the end of it?

[redacted] do we need to take a short break?

COURT REPORTER: Five minutes would be fine.

(Recess from 1:07 p.m. to 1:21 p.m.)

THE COURT: Let's continue. I want to move to the Fourth Amendment, but by moving to the Fourth Amendment, I'm not really totally moving away from a statutory assessment of targeting. Both of them have a reasonable component in the statutory targeting assessment that may be a reasonably designed component, but in the Fourth Amendment, there's also much more

of a reasonable aspect.

We've assumed, in prior 702 dockets, that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications and therefore that the acquisition of electronic communications can result in a search or seizure within the meaning of the Fourth Amendment. Consistent with the position that it's taken in other matters before the FISC, the government does not assert otherwise in the multiple filings in this matter.

Can the Court infer, therefore, that the government does not disagree with the proposition that the acquisition of electronic communications can result in a search or seizure within the meaning of the Fourth Amendment?

[redacted]: I think so.

THE COURT: All right. I'll take "I think so" as a yes.

(Laughter)

[redacted] I'll clarify my remarks for the record. Yes.

THE COURT: Let's talk about incidentals. The government's position is that the collection of wholly domestic communications as part of the Internet transactions that NSA acquires through this upstream collection is incidental for purposes of the Fourth Amendment.

Now, as the government acknowledges, the mere fact that an

intrusion is incidental does not necessarily render it reasonable and thus permissible under the Fourth Amendment, and I think you've acknowledged that in one of the June submissions, the June 28 submission probably.

And then in the August 16 submission, it's indicated that, as we've talked about, that NSA acquires at least 2,000 to 10,000 transactions annually that contain one or more wholly domestic communications that are not to, from, or about a task selector, at least that's what this statistical analysis shows.

Now, do those numbers alone establish a fairly substantial intrusion on the protected Fourth Amendment interest, particularly when you consider that the actual number of wholly domestic communications may be higher depending upon how convincing you are in a further assessment of the unknown category of communications, also considering that each transaction may actually contain multiple communications, and also taking into account that many of the persons whose communications are being acquired have little or no connection to the user of the task selector?

Some persons outside the United States are protected under the Fourth Amendment, and also we don't know what this category of *about* communications in the four to 5,000 of the 50,000 that were set aside as being discrete communications will turn up.

Just in terms of the numbers, it looks like there's a fairly substantial intrusion on protected Fourth Amendment

interest, doesn't it?

[redacted]: I think that's right, Your Honor. I think there is clearly an intrusion upon Fourth Amendment protected interest, but in conducting the Fourth Amendment balance, we also have to consider the protections that are put into place to protect those Fourth Amendment interests.

And as we've asserted, we're committed to destroying any wholly domestic communications that, for whatever reason, have run through NSA filters and happen to land in an NSA repository and are recognized by NSA analysts as such.

So, yes, even though the Fourth Amendment intrusion may be greater, we are taking basically the ultimate step that we can in minimizing the effects of that intrusion by destroying any MCTs that have wholly domestic communications within them.

THE COURT: And part of the assessment, of course, is a balancing assessment under the Fourth Amendment that looks, as we're considering the certifications and the procedures and whether they satisfy the Fourth Amendment, the government would stress the importance of the upstream collection to national security.

I want to just assess that a little bit and get a little bit more of a sense of that. Just numerically, the collection of Internet transactions really is a pretty small part of the collection as a whole. We're not talking about telephonic communications, and according to the numbers, the upstream

collection in the aggregate only constitutes about 9 percent of all Internet communications acquired pursuant to 702. We have the PRISM collections, etc.

And then based on the sample and the analysis applied, only 10 percent of that 9 percent, which results in .9 percent, or .009 of the overall collection of Internet communications is Internet transactions containing multiple communications.

That would suggest that the collection of Internet transactions through the upstream collection, and particularly the MCTs that we're concerned about, isn't a particularly critical national security tool. It's a really small part of what NSA collects. Why should I conclude that it's so vital, looking at that side of the balance?

MR. INGLIS: Your Honor, I would offer and then pass to [redacted], perhaps [redacted] from the operational side of the house, two points. One is that it uniquely covers a scene [redacted]

[redacted]

THE COURT: [redacted]

[redacted].

MR. INGLIS: [redacted]

[redacted].

The second is that this collection [redacted]

[redacted].

So a significant percentage of our counterterrorism reporting is ultimately attributable to what we do in 702, and albeit the percentages would show that the upstream is a relatively small percentage of that, but it covers a unique scene [redacted] we can't get other ways.

[redacted]: With respect to technology parsing out those MCTs, we don't have the technology to eliminate the MCTs without also eliminating the bulk of the discrete communications. We'd lose all of that except for [redacted] that we fully understand.

THE COURT: This is a unique Fourth Amendment context, as many legal settings will be unique, and therefore, the Court,

I am having some difficulty in assessing just how the balancing under the Fourth Amendment is applied. But if the primary value of the upstream collection is the acquisition of a fairly small number of communications that have high value to national security, how does the Court balance the possibility of such acquisitions against the known acquisition of at least thousands of nontarget communications each year?

Another way of putting it would be, does the possibility that NSA is going to acquire a single piece of valuable intelligence outweigh the privacy interest of these thousands of U.S. persons and persons in the United States whose communications are being incidentally, if you will, acquired?

How do I make that assessment and reach that balance? Is the intelligence value always going to rule the day? Is one valuable piece of intelligence enough to justify the thousands of Fourth Amendment intrusions that are involved here?

[redacted]: Your Honor, I think what was demonstrated in our sample, and I want to perhaps correct a statement there that we get relatively few communications through upstream collection that are of intelligence value. I think what our sample showed was that we get millions of Internet communications that are of potential intelligence value and a very small number of those which have the potential to be wholly domestic.

MS. MONACO: I think I would follow up on that, Your

Honor, by saying that the Court has posed, I think -- put it in somewhat more of a starker context than I think the government has in its filings. In other words, the Court has already acknowledged that the FI, or the foreign intelligence information sought through the to, from, or about task selectors is of paramount importance to the government and is of the highest order of magnitude. I think that is the one side of the balance that the Court is faced with, and we would not suggest that it should be put in such stark terms.

In other words, on the other side of the balance, what we've tried to do in the study that NSA has done is indicate the relatively small portion, understanding the questions that the Court has raised at the beginning of the hearing about those numbers, but we've tried to put in place a series of measures that would enhance the ability of the Court to make its reasonableness finding in terms of the analysis that gets done as the information is seen by the analyst.

So I would suggest to the Court that, no, setting one potential piece of foreign intelligence information against the privacy interest of potentially thousands of domestic communications is, I respectfully suggest, not the appropriate analysis but rather the paramount interest of the foreign intelligence contained in those MCTs and our inability to get at that paramount important information other than by collecting the whole MCT.

Balance that against the procedures and the number of steps that the government is proposing to be put in place to ensure that there is the maximum amount of privacy protection that can be applied to those potentially problematic pieces of communications.

THE COURT: Would we all agree that ultimately the assessment or application of this balancing under the Fourth Amendment might be different depending upon whether they're in this fairly substantial upstream collection that is still a limited percentage of the total collection but the outcome of the Fourth Amendment balancing might be different depending upon whether the collection of wholly domestic communications was 1,000 a year, 10,000 a year, 100,000 a year, 10 million a year?

It would depend upon what those numbers show, if you will, that at some point the collection, even though unintended or incidental, at some point the acquisition of a large volume of Fourth Amendment protected communications would simply be too much under the Fourth Amendment? Would we all agree that there is some tipping point?

MR. INGLIS: Your Honor, I would agree from an NSA perspective that there is. In the extreme, there must be a line. It's probably not objectively determinable, but there would be a line. If the preponderance of material that we picked up was in fact wholly domestic or declared incidental but in fact it was the preponderance of what we picked up, clearly

we'd be in the wrong place.

THE COURT: I think that's a good way to put it, Mr. Inglis, that if you have a preponderance that's in the wrong category, then maybe that would be too much.

MR. INGLIS: So if I might, given the opportunity to answer the question in a subjective manner, complement Ms. Monaco's answer, I would offer three things as to whether this achieves a reasonable balance between those competing concerns.

The first is that it does offer unique material that we believe could provide valuable foreign intelligence. If it were not unique, if we could in fact make up for this some other way and given the problematic nature of this, I think that we would quickly go to that corner, but we haven't found another way to go after what we see as unique material.

The second is that we've taken what we believe are all reasonable measures in the technology and a set of then equally, if not more so, reasonable procedures of how we then use the fruits of what that technology provides to address the real and material concerns about Fourth Amendment, statutory, or the Court's authority, have we made reasonable use of that such that we are focusing the majority, the preponderance of our efforts after the greater purpose and at the same time an equal amount of time and effort to make sure that we don't then incidentally or intentionally collect the wholly domestic.

The last thing I would say is that in equating whether one report is the equal of or is offsetting against incurring intruding upon the privacy of thousands of individuals, that's a hard call, but the one report could in fact protect millions of individuals, depending upon the density of the population it is under, is it at risk, and what that report might pertain to. So that's the great unknowable here is how valuable is that single piece of intelligence.

THE COURT: One could use that accurate observation to support the conclusion that one piece of intelligence does outweigh whatever the Fourth Amendment intrusion is, and I think if most reasonable people actually weighed that one piece of known intelligence that would save millions of lives against any number of Fourth Amendment intrusions, they'd say, yes, get that piece of intelligence.

MR. INGLIS: I would argue that, sir, but I would not be completely impartial in making that argument.

THE COURT: All right. Just one or two small questions, and that will be the end of this inquisition. Is NSA able to acquire [redacted] that are to, from, or about a task selector from a service provider?

[redacted]: Yes, we are.

THE COURT: So, what would NSA acquire in the upstream collection in those categories that could not be acquired from the provider, anything?

[redacted]: What could we obtain from, for instance, [redacted] from the upstream world that we couldn't obtain from the provider?

THE COURT: Right. Do you get anything more through the upstream collection [redacted]

[redacted]: Yes. [redacted]

[redacted]: Your Honor, if I may, just to take this up another level of generality. In general, NSA cannot do *abouts* collection at the ISP, so that [redacted] that would be entirely off the table, [redacted]

[redacted]: I also need to add that we do not obtain

abouts collection from [redacted].

THE COURT: Okay. So back to the evolution and the dynamic nature of the Internet, and I'm curious as to how this phenomenon affects the Fourth Amendment balancing given that the upstream collection is going to be constantly changing because of the nature of the Internet.

If the government can't predict just what the impact of any changes in the Internet will be on the collection, is it valid for the Court to presume in a Fourth Amendment analysis that the scope and intrusiveness of the upstream collection will expand or contract or stay the same?

What should the Court presume in applying a Fourth Amendment analysis? Just take it as it is frozen now, or is it valid to make some presumption or assumption with respect to the future given what the experts see with respect to the Internet and its evolution?

MR. INGLIS: I'll leave it to my Department of Justice colleagues to speak on the Fourth Amendment implications, but I would say that the Court can and should assume that it will change. I don't know whether to the greater or the lesser benefit of the interest between the government and the Court, but it will change. And I think the expectation of the Court upon the government is that the government will discern that change and faithfully either stay within the authorities granted

by the Court or come back to the Court and argue that those authorities must be modified in some way, shape, or form based upon those changes.

THE COURT: So, in this setting, with the certifications and the Fourth Amendment, if the Court is comfortable, based on the record before it not withstanding the fact that there will be changes, there will be evolutions, the Court should simply rely on the renewal process and the obligation of the government to come forward with any additional information, changes in the technology or what have you, in order to assess a future certification.

MS. MONACO: Your Honor, I would add to that that certainly the Court should rely on that, but I would add to that the Court should also hold the government, quite obviously, to the procedures that we've discussed would apply in this case precisely because we understand the evolving nature of the Internet, precisely because we understand the real, and I would say nontrivial, intrusion that we've all acknowledged and discussed here, given the nature and collection of MCTs.

And it's precisely because of that that I think the government would propose to put in place these series of steps in what I guess we've termed a multilayered approach to try to do the utmost in terms of being able to enhance the privacy protections that exist in the existing minimization procedures that can be applied to that potentially problematic collection.

THE COURT: All right. Any other questions legal advisors have?

[redacted] Yes. Can I just ask one quick question? Do you have a rough estimate as to the percent of Internet transactions that are actually handled by [redacted] just a rough? No? Lots? Few? Anything?

THE COURT: Certainly you've said that because of the place of the United States in the Internet, there's a very heavy use of --

MR. INGLIS: So two things remain true, which is the majority of the world's reliable communications continue to flow through the United States, largely because of the investments made over the last 40, 50 years in the creation of the Internet and also because of the inherent stability, resilience of the infrastructures that then underpin that.

There's also a degree of innovation that continues to center on the United States, and despite its best efforts, China, Russia, others, have not yet created the engine of innovations that have taken those products and materials offshore, but that has begun to occur.

So you do see a flattening of the innovation, you see a slight flattening in terms of the infrastructure. So today, and I think for the foreseeable future, the preponderance of communications are still centered in through the United States. But I can see a world 50 years from now where that might be

completely flat. I can't predict that far out. I just know over the next year or two we can depend upon the trends that extend from 10 years past.

[redacted] And another thing we can say which may be obvious, with respect to our targets, particularly [redacted].

MR. INGLIS: And I've been pleasantly surprised from an intelligence perspective [redacted]. I would never have predicted that 10 years ago, and yet it's been extraordinarily lucrative for us.

THE COURT: All right. Any other questions?

So, let me make one or two observations, and we'll talk about what further you can provide. And I do note that I've kept you here for a long time, and I do know that some among you may have other places to get to.

It seems to me that to the extent that either the statutory or the Fourth Amendment analysis turns on the record and statistics, if you will, and numbers of potential or actual wholly domestic communications that are acquired, things of that sort, we have a situation where we have this -- I'll call it fairly low number, at least in terms of percentages, of between 1 and 5,000 every six months having identified through your

statistical analysis as containing wholly domestic communications that are to, from, or about a task selector.

We then have a larger category that I refer to as "unknown" that is identified as between 48,609 and 70,168 every six months that you've indicated you've made some assessment of that takes you out of the category of totally unknown and into a category of highly unlikely, at least, or whatever term you want to apply, or can under the facts apply, highly unlikely to contain wholly domestic communications.

I'm not yet convinced that the record before me supports the conclusions that have been articulated. So I will look for further information on that to bolster that assessment.

We also have this other category, in your random sampling again, that is 9/10ths of the random sampling that was set aside as being discrete communications -- 45,000 out of the 50,000 -- as to which our questioning has indicated we have a concern that some of the *about* communications may actually have wholly domestic communications.

And I don't think that you've really assessed that, either theoretically or by any actual examination of those particular transactions or communications. And I'm not indicating to you what I expect you to do, but I do have this concern that there are a fair number of wholly domestic communications in that category, and there's nothing -- you really haven't had an opportunity to address that, but there's nothing that has been

said to date that would dissuade me from that conclusion. So I'm looking there for some convincing, if you will, assessment of why there are not wholly domestic communications within that body which is 9/10ths of the random sample.

Those things, and anything else that we identified, really was right at the outset of our discussion today, it would be very helpful to receive any further information on those. We don't have much time, though.

So I think in fairness to the Court, which is very constrained in the time available now to resolve and write up any resolution, particularly if I conclude that I cannot totally approve the certifications, you need to get that to me as quickly as you can. I have to say even this week. It would be very difficult if we didn't have it this week to formulate and frame the resolution of these matters and get it committed to writing.

Anything else you want to say I would be happy to receive, and I don't want to give the impression that this is the last point of communication even in addition to the written response that you may have in the next couple of days. If there's more to be discussed, then the Court is, in the words of Ross Perot, all ears.

MR. INGLIS: Your Honor, if I might ask a question regarding your summary, you had said at the outset of the conversation expressed a possible concern that the purged data

might constitute an unexplored piece of the territory, to the extent that it would be useful for us to describe the attributes of those things purged and for what reasons, we'd be happy to provide that as well.

THE COURT: Anything you can provide on that, which really goes not to the -- well, it goes to sort of a generalized assessment of the validity of the representative sample.

MS. MONACO: Your Honor, if I might suggest, we understand the constraints on the Court's time on this, and we very much appreciate all the opportunities the Court has afforded the government to provide it additional information.

I think what we will do is go back and confer and ensure that we can provide you whatever it is along these lines that we can by the end of the week and be in touch if the Court permits with the legal advisors on the precise timing on that.

THE COURT: They are always open to such communications.

MS. MONACO: And then what I would also say is I know we've had some of this contact I think at the staff level, but looking ahead I think we'll also be in touch on potential coordination of any transition should the Court be poised to issue an order.

THE COURT: We understand the significance of the collections and the significance of technological and other issues with respect to any modification in what is currently

being done, and we'll try to be as open as reasonably possible.

MS. MONACO: We appreciate that.

[redacted] Your Honor, earlier in the hearing as well you had asked where a particular part related to the unknowns --

THE COURT: I'm sorry, what?

[redacted] I'm sorry. You had asked where some of the representations we had made here today with respect to the unknowns was in relation to the record indicated that some of those points were captured in the 30 August submission. I would point the Court to the final paragraph on page 6 of the 30 August submission there for a few of those representations just for reference.

THE COURT: And certainly, I hope you don't think that we didn't look at and take fully into account the August 30 submission, but I think you can also conclude that it wasn't fully convincing, so anything more you can do to convince would be appreciated.

All right. Thank you again for coming and putting up with these long proceedings. I'll let you get on your way. I'll look forward to receiving further information and to talking with you along the way in resolving this very important, unique, and in some ways difficult matter. I thank NSA and the Department of Justice for all their efforts in this regard. Thank you all. (Proceedings adjourned at 1:52 p.m.)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu