~~SECRET~~

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

~~SECRET~~

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

SECRET

United States Foreign Intelligence Surveillance Court of Review

In re: Directives to Yahoo, Inc. pursuant to Section 105B of the Foreign Intelligence Surveillance Act) Case No. 08-01

BEFORE: The Presiding Honorable Bruce M. Selya
Honorable Ralph K. Winter, Jr.
Honorable Morris S. Arnold

United States District Court
Courtroom No. 3
One Exchange Terrace
Providence, Rhode Island
June 19, 2008, 10:30 a.m.

[redacted] RDR, CRR
Official Court Reporter
United States District Court
595 Main Street, Room 514A
Worcester, MA 01608-2093
[redacted]

Mechanical Steno - Transcript by Computer

SECRET

Present:

Gregory G. Garre, Acting Solicitor General
J. Patrick Rowan, Acting Assistant Attorney General
Mathew G. Olsen, National Security Division
[redacted] Office of Legal Counsel
National Security Division
for the Government

Marc J. Zwillinger, Esquire
[redacted]
Jacob Summers, Law Clerk
[redacted]

I N D E X

PROCEEDINGS

THE CLERK: The Honorable Court. All rise.

The Honorable -- the United States Foreign Intelligence Surveillance Court of Review is now in session. All persons having any business before the Honorable Court may draw near, give their attendance, and they shall be heard. God save the United States of America and this Honorable Court.

You may be seated.

JUSTICE SELYA: *Good morning.*

THE CLERK: Case No. 08-01, in re: Directives to Yahoo, Inc. pursuant to Section 105B of the Foreign Intelligence Surveillance Act.

Each side is allotted 45 minutes for argument.

JUSTICE SELYA: You may proceed, Counsel.

MR. ZWILLINGER: Good morning. May it please the court, my name is Marc Zwillinger, and I appear on behalf of Yahoo. I would like to save 15 minutes of my time for rebuttal.

JUSTICE SELYA: I'm afraid that's -- that's a bit too long. We'll allow you to reserve five.

MR. ZWILLINGER: Okay. Thank you, your Honor.

JUSTICE SELYA: That will be deducted from your opening time.

MR. ZWILLINGER: Obviously, this is a highly unusual

case, and it comes on an unusual posture, because there was no hearing, nor was there argument below. So, I would like to start by making a few initial observations that I think would be of substantial assistance to the Court in deciding the issues before it. And the first has to do with the nature of the surveillance at issue.

I have been representing Yahoo on government compliance matters for six years; and before that I was a government prosecutor myself, with a top secret security clearance in the computer crime section of the Department of Justice. I requested surveillance, and I've read the fruits of surveillance. Neither I, nor Yahoo, have the naive understanding of the importance of surveillance, the government's mission in protecting this country.

JUSTICE ARNOLD: Counsel, could I ask before you talk about that part about the jurisdictional point, assuming that -- that we were to decide that your opposition to the motion to compel was not an application within the meaning of the statute, what is your -- what -- what's your jurisdictional basis for being here?

MR. ZWILLINGER: Well, you put your finger on the one point in the case where the government and Yahoo both agree, which is that Yahoo's opposition --

JUSTICE ARNOLD: They agree, but they can't confer jurisdiction on the Court.

MR. ZWILLINGER: That's right, your Honor.

JUSTICE ARNOLD: And also they said that the reason they've agreed was that if they lost they thought they would be arguing that we would have jurisdiction over a petition from them, and that's not -- that's not a legal reason assuming that we have jurisdiction.

So what is your jurisdictional basis?

MR. ZWILLINGER: The jurisdictional basis, your Honor, is that our opposition to the motion to compel should be treated like a petition for purposes of appellate jurisdiction. That is to not treat it as a petition would elevate the form of it over the substance. We could have titled our --

JUSTICE ARNOLD: What part of the statute would give us jurisdiction?

MR. ZWILLINGER: 1805B(i) would jurisdiction over a petition.

JUSTICE ARNOLD: Does that require a petition to be made to this Court within a particular time?

MR. ZWILLINGER: The statute doesn't require petition to be made in a particular time. The draft rules for the Foreign Intelligence Surveillance Court specify promptly, but the statute itself doesn't require the petition to be made in any certain period of time after the directives are received.

JUSTICE ARNOLD: But this says not later than seven days after the issuance of a decision; isn't that right?

MR. ZWILLINGER: Well, we did file our petition for review not later than seven days after the issuance of the decision below.

JUSTICE ARNOLD: That's what I want to make sure. Thank you.

MR. ZWILLINGER: Yes, we did. So, where I thought I -- it was worthwhile to start is to talk about the nature of the surveillance, because this is unlike any surveillance that takes place under any other statute, and I have brought with me, which I think the Court would benefit from, to view the tasking orders that Yahoo has received. This is something we could not have presented to the lower court, because we did not receive them until after the lower court asked -- insisted that we comply with the directives.

JUSTICE ARNOLD: Well, I'm sorry to interrupt you again, Counsel, but let me ask you another question, I think is prior, at least as a logical matter in my mind, and this is the issue of standing. What is your injury?

MR. ZWILLINGER: Well, our injury, your Honor, is that we're being forced to redirect our resources to compel with what is an incredibly broad and pervasive surveillance regime.

JUSTICE ARNOLD: Doesn't the statute compensate you for that?

MR. ZWILLINGER: It does.

JUSTICE ARNOLD: Don't you get compensation?

MR. ZWILLINGER: But the compensation that it provides in terms of financial compensation doesn't compensate us for the full injury that we suffer. One of the most important things that people use Yahoo for is they understand that their private communications will go back and forth between -- on -- between their --

JUSTICE ARNOLD: Well, if this order is enforced and it's secret, how can you be hurt? The people don't know that -- that they're being monitored in some way.

How can you be harmed by it? I mean, what's -- what's the -- what's your -- what's the damage to your consumer?

MR. ZWILLINGER: Well, generally, your Honor, I think the perception that widespread wiretapping is a trend under the PAA is well known without having --

JUSTICE ARNOLD: Well, that is true whether we enforce this order or not; isn't that right? The perception would still be there, so the market's already discounted for any injury that you might have -- you might suffer.

MR. ZWILLINGER: Well, I think there's two components to the injury. The first is -- the compensation -- financial compensation for complying with the government's order does not compensate us for the injury of participating in the surveillance. We are being asked and compelled, we believe, to participate in surveillance that we believe violates the Constitution of the United States. If that is so, that is an

injury.

JUSTICE ARNOLD: Would an injury give you standing?

MR. ZWILLINGER: I certainly believe it is, your Honor. We are being asked -- we are being --

JUSTICE ARNOLD: Well, I would like to make just one more point and let you go on. If, in fact, you're being injured by what you call a perception among consumers that their privacy might be being violated, that's true of all your competitors, too, isn't it? So, what -- you don't really have a competitor here, do you?

MR. ZWILLINGER: Well, according to the government, [redacted] but I would --

JUSTICE ARNOLD: So, I guess people might be using other forms of communication; they might be substituting mail or something like that. Okay.

MR. ZWILLINGER: If I might, your Honor, I think the Court would significantly benefit if I could pass up to the clerk copies of the tasking orders that we've received. I have copies for the government as well. These are redacted, of *course, to obscure the identity of the* [redacted] *at issue.*

What I've handed the Court is a tasking order. This is what Yahoo receives from the government. When the directives say that [redacted] the government will [redacted]

they mean that since [redacted]

You're looking at [redacted] list that identifies to Yahoo the e-mail accounts that are supposed to be placed under surveillance; and [redacted]

[redacted]

Why I show this to you is because I think it's a perfectly fair question for you to ask the Solicitor General of the United States how a name gets on this list. This isn't reviewed by a -- the FISA Court. These names aren't reviewed by the Attorney General of the United States. The difference between surveilling an account and exposing someone's most private communications and not is how a name gets on this list; and all we know about it from page 47 of their brief, is that an intelligence analyst puts it on the list.

[redacted] of the accounts we have been given do not exist. They aren't accounts at Yahoo. Whether the government is misinformed, or using stale information, we don't know. But the fact that [redacted] accounts do not exist raises a

serious possibility that some of those accounts have already been recycled and are used by other Yahoo users, or that the information that the government has is just wrong, and the wrong account is being placed under surveillance.

I make this point also, because in reviewing the cases, I read the concurrence in the Keith opinion by Justice Douglas, and he said he was aghast at the notion that 900 conversations had been intercepted under the warrantless domestic surveillance.

We are just one provider. We have [redacted] accounts placed under surveillance in [redacted]. That's the magnitude of the surveillance we're talking about. I think that does lead to the impression that widespread surveillance is rampant under the PAA.

The other thing I wanted to talk about is the location of the surveillance, because even though you can't tell this from reading the lower court opinion, the surveillance is being set in the United States, in Sunnyvale, California, by the same team of compliance paralegals that set surveillance for Title III orders, or for FISA orders.

Why is that important? Because the cases like United States versus Bin Laden that talk about the difficulties of getting a warrant for foreign intelligence information talked about it in the context of the difficulty of dealing with foreign law enforcement, or the difficulty of serving a warrant

on a foreign provider, and the lack of jurisdiction, but this is right here in the United States, which leads me to the more important point, and the one most significant mistake the FISA Court made. If the government mistargets, the consequences of that will be felt here in the United States by a United States person. This is not a phone exchange in Abu Dhabi where if they're off by one digit, they're likely to get a different telephone user in Abu Dhabi, who's not likely to be a U.S. person.

The difference between a U.S. person and a non-U.S. person in this context could be a letter or a digit in an email address; and if they have it wrong, the consequences will likely be felt here, because more Yahoo users are from the United States than any other single country.

JUSTICE WINTER: And what will such a user feel?

MR. ZWILLINGER: Because of the surreptitious nature of the surveillance, they wouldn't feel anything. Their accounts would be surveilled. Their private communications would be disclosed. [redacted] They would make their way on to some government list.

JUSTICE WINTER: Aren't the -- aren't the probabilities that whoever saw these communications in the government isn't there a probability that that person would have no idea who it was that sent them and would have absolutely no use for them, and that it would be an enormous

coincidence if by chance somebody would recognize it?

MR. ZWILLINGER: No, I don't think that's right, because [redacted] and the communications themselves often contain private revealing data about who is sending it; that is, when you send an email, your signature is often at the bottom of it.

JUSTICE WINTER: Yeah, but if I'm somebody who's looking at this, and it's John Jones in Jacksonville, Florida, and I -- aren't there procedures under which this can't be retained? I mean, how likely is it that we're going to have any use whatsoever, that anyone would have any use whatsoever, of information in the state that can be counted?

MR. ZWILLINGER: That's an excellent question, your Honor, and I would ask you to ask the Solicitor General for two reasons. One is part of the procedures are redacted, and we have not had a chance to see them.

JUSTICE SELYA: Yeah, but you know there are minimization procedures.

MR. ZWILLINGER: But the minimization procedures don't prevent the -- all subsequent use of the information. In fact, Congress when they're looking -- they've been looking at redoing the statute, right, because the PAA has lapsed. If you look at the Senate report that the government cited with regard

to the new statute, Senate 2248, which has not yet been passed, the Senate report says one of the problems with the PAA is there weren't restrictions placed on the government as to what they could do with the information once they obtained it.

So, to the extent you are questioning how the government can use the information, I'm not the authority.

JUSTICE WINTER: I'm questioning it, because you -- you are telling me -- you did tell us that there were consequences being felt by individuals in the United States, and that seems to me far from clear in these circumstances. It seems to me it would be highly unlikely there would be any consequences if they got -- by mistake got into my email account, even if I had something on there that would be even in the remotest interest to anyone else, so what? They don't know who I am, or anything about it, and there are minimization procedures. So it seems to me, you know, you're talking about very abstract -- very abstract harms.

MR. ZWILLINGER: I have -- I have two responses to that. One is I don't think the case law suggests that an intrusion into someone's privacy, an invasion of their communications, a ransacking of their private papers is harmless if the government makes no further use of it. I think the case law says the exact opposite. I think it says that there is privacy intrusion felt by individuals, harm to individuals when their privacy is intruded upon, even if the

government makes no further use; but second, I think the government would concede --

JUSTICE WINTER: No, but a lot of those cases are going to be people, who are not targets of search warrants; for example, who are in an apartment, and their privacy was invaded when the people with the warrants came in, and they are there being physically intruded upon. The people you're talking about don't even know that -- that an email may have been read by somebody.

MR. ZWILLINGER: I think the juris prudence about surreptitious entry is even more exacting than the juris prudence with a knock and announce. That is when you want to tell somebody you're going to their house, the standards are lower than when you want to do it on a surreptitious basis, because we think the surreptitious intrusion into privacy is one of the --

JUSTICE WINTER: The standards may be lower. I don't want to prolong this, because you only have so much time, but I'm just having trouble seeing who exactly is being hurt here, other than -- than people, who understandably, perhaps, like to feel comfortable in knowing that -- that we have a rigid Fourth Amendment protection of individuals and don't want to even contemplate that people are having their privacy unknowingly intruded upon.

MR. ZWILLINGER: I guess one response on the

theoretical harm and then another practical point. I would just point to Justice -- I would just point to the Berger case, because in Berger and Katz, you know, the Supreme Court said that these intrusions on wiretapping without any subsequent discussion of use, but wiretapping individuals' private communications is the greatest harm an individual can experience; and I understand your point that they don't know they're experiencing that harm, so it can't be that great, but the government building a database on millions of people in the United States, even if they don't know it, I would argue would be a grave harm. But specifically, I would say that the government is not -- my understanding is they're allowed to retain information.

JUSTICE WINTER: Now you're getting close to a real harm, the government building a database, including large numbers of individuals, who are mistakenly surveilled upon. I will ask the Solicitor General if that's happening.

MR. ZWILLINGER: And you can also ask him if isn't it true that they can --

JUSTICE WINTER: I may forget to ask him. I would like to hear his answer anyway.

MR. ZWILLINGER: The materials can be retained and used by the government under certain circumstances. I'm not as fully versed on those circumstances, other than if they show commission of a crime, even though you were not reasonably

under surveillance to begin with, even if there was no suspicion that you were involved in a crime, if they see that you were involved in a crime they can make further use of that material. So, the other use would be that if they surveil lots of people and find evidence of crime, they now can use that information in all sorts of ways against that person when the Fourth Amendment would have required some particularized showing. At least it's my understanding.

JUSTICE SELYA: The problem that I'm having, Counsel, with your -- with your argument is that we start the premise that this statute does not require the -- the individualized warrant that is so characteristic of -- of our typical Fourth Amendment juris prudence, all right. If -- without that individualized warrant requirement, we're always going to have some incidental over -- over -- overdisclosure. As long as that isn't intentional, as long as there are procedures in place for minimization and for how the government constructs the certification that's required by the statute, I'm struggling with the notion that -- that you're doing anything except trying to get us to incorporate the characteristics of a warrant requirement into a statute that doesn't require a warrant to begin with.

MR. ZWILLINGER: It's an excellent question, your Honor, and let me try to address it in a couple of ways. First, set aside for the moment the question of whether we're

under some sort of exception to the warrant clause. I think there's reason to say we're not, but setting that aside, assuming we are. Fourth Amendment juris prudence suggests that in determining the reasonableness of a surveillance, you don't ignore the principles of the warrant clause. It's not putting a back door warrant requirement in to say if you're going to do warrantless surveillance, you still need to do it consistent with reasonableness. And this Court, in 2002, looked at the question of how you determine something is reasonable even under the circumstances where it believed the warrant clause did not apply. And it went and found three principles drawn from the Fourth Amendment that you look at, even if a technical warrant is not required, and the three principles were: The three Ps, prior judicial review, particularity, and a probable cause finding.

JUSTICE ARNOLD: Let me ask you about that, about your first P. What is the effect of the power of the FISA Court under the -- under FISA to approve the procedures that the government has proposed?

MR. ZWILLINGER: All those --

JUSTICE ARNOLD: Is there some kind of prior judicial activity that would satisfy that?

MR. ZWILLINGER: I don't believe it is, and here's why. Those procedures that they're to approve are to determine whether the person is located outside the United States, but

that is not a proxy for whether they have Fourth Amendment protection. Being outside the United States does not waive your Fourth Amendment rights. When you travel for two weeks to Italy on vacation, you are as protected against our government under the Fourth Amendment as when you are here. So being overseas, which is the finding the Court reviews their procedures to determine if they're overseas, that's not a relevant prior judicial review, but Congress seemed to use that as a proxy either for that or as a proxy for the fact that because they're overseas, they're using an overseas facility to communicate, but in the case of directives served on Yahoo that's not the case. They're using a U.S. facility to communicate. So I don't think that prior judicial review is sufficient.

The second one is particularity, and going back to the point I made about where the court erred below. If this Court follows its own holding from 2002 that particularity is an important component of reasonableness even where a warrant is not technically required, there's no particularity finding being made here. The way a name gets on this list, the way we have [redacted] names under surveillance, there's no requirement that the government show linkage between these email accounts, these facilities, and an agent of a foreign power. There's certainly not one that they have to show to a court. If they have some redacted procedures that we haven't seen, we don't

know what they are, but they say an analyst puts it on this list.

And the third P we talked about is probable cause. And if you look at the case law, FISA itself was challenged as being unconstitutional many times. I've reviewed at least ten decisions. We cited four or five in the brief. It starts with the United States versus Duggan in the Second Circuit, and Cavanaugh, and a whole series of cases that says FISA is constitutional. The reasons they say FISA is constitutional all go back to these three Ps. They go to the role of the FISA Court in approving a finding of probable cause that the U.S. person was an agent of a foreign power; or they go back to the FISA Court approving a particularity showing; and if you took away those things, the way the Protect America Act has taken them away, I don't think any of those decisions come out the say way, least of all the decision in In re: sealed case. The three Ps was the focus. Yes, the Court talks about minimization. Yes, the Court talked about duration, but it said it specifically that other courts have said that these have constitutional significance. The FISA Court here placed all of their eggs in the minimization and duration basket.

JUSTICE ARNOLD: What exactly was the scope of the FISA Court's approval of the government's procedures under the statute?

Okay. Do you know what I'm talking about?

MR. ZWILLINGER: If you could.

JUSTICE ARNOLD: The statute requires the government to produce to the FISA Court procedures under which they are going to intercept these communications, and the FISA Court has a certain amount of time within which to approve those procedures.

MR. ZWILLINGER: Right.

JUSTICE ARNOLD: So what -- what was the effect of that?

MR. ZWILLINGER: The only procedures that the FISA Court would be approve would be the targeting procedures, how they determine that someone is out of the country, and the minimization procedures.

JUSTICE ARNOLD: And minimization?

MR. ZWILLINGER: And minimization. And we're not arguing about minimization. The FISA Court said they use the same minimizations they use under FISA orders. We're not arguing about that.

What we are saying is minimization and particularity go hand in hand. Minimization is what prevents after there has been an intrusion in privacy from that intrusion to continue to be magnified throughout the government.

Particularity prevents the innocent U.S. person sitting at home from having their account looked at, and there's no particularity here. There's just minimization.

So --

JUSTICE ARNOLD: Sitting at home not abroad?

MR. ZWILLINGER: Sitting at home, if they have the email account wrong, that person will be --

JUSTICE ARNOLD: Well, leaving that to one side, well, that's -- I mean there are other concerns, are there not, as to with the Fourth Amendment rights to citizens abroad?

MR. ZWILLINGER: Well, the particularity concern, the one that's so much animating this discussion is that if there is not a required showing to the FISA Court that the account is being used by the agent of a foreign power then there's no check to make sure they're surveilling the right account.

JUSTICE ARNOLD: Well, what is there in the record that indicates that there's a large error rate?

MR. ZWILLINGER: Well, all we have, and again, this is an unusual case, so we have the tasking orders that we received after the FISA Court ruled.

JUSTICE ARNOLD: Those are not -- those are not in the record; is that right?

MR. ZWILLINGER: We had no -- they're not in the record, but I'm representing to you that we have [redacted] accounts that do not exist that are appeared on these tasking orders.

JUSTICE SELYA: Right. But there's no harm from those errors, if those accounts don't exist, they obviously can't be invaded?

MR. ZWILLINGER: That's right, your Honor. I'm not arguing that those [redacted] caused harm. I'm saying those [redacted] are indicative -- they're indicative of a problem. The problem is that when the government has to go to the FISA Court and make a showing, they have to show that the account they want to surveil is likely to be used by an agent of a foreign power, and that's a check on them. That's a verification that they're surveilling the right account the same way in which normal criminal surveillance requires them to show to a court that the address is where a crime is likely to be committed so they know they're surveilling the right address. And what we're saying is the [redacted] is indicative of a problem. The [redacted] we're getting is indicative of a problem.

JUSTICE WINTER: Why is it so clear that having a requirement that the FISA Court review whatever it is the government people review, how do we know the FISA Court isn't going to make the same [redacted] mistakes. It may be the information that the government has that led them to target a particular account is -- is information that turns out to be wrong, maybe disinformation, it can be any number of things in this area. How do we know that -- why do you think the FISA Court is going to discover these errors?

MR. ZWILLINGER: Well, I think there's two responses. One is I do think the government is forced to make some sort of showing to a court before it initiates a surveillance that it

will be a check on the process. It will be a diligent check on the process. I think the government is going to stand up here, the Solicitor Generals, and say we do that, we just do it ourselves. We don't show anybody else.

JUSTICE WINTER: Well, that was what I was going to ask you. Are you -- are you really saying that even if the statute said these procedures must be in place, the Attorney General must make the certification, the government must say it has complied to procedures, and there's a requirement then you must put what you have what the government had before the FISA Court, the procedures, the information for -- for the FISA Court to see do these things match? Are you saying it's still unconstitutional?

MR. ZWILLINGER: Well, one, I'd say that we have nothing. The statute doesn't provide any of these things. If you're asking me hypothetically what would the problem then I would say we get to the problem, the fundamental problem, that's about their Executive Order 12333.

JUSTICE WINTER: Well, I'll put it more bluntly, are you -- are you saying that someone should check on whether the government is telling the truth?

MR. ZWILLINGER: I'm saying someone should determine not that they're telling the truth, but that there has been some linkage between the U.S. communications facility account to be surveilled and the agent of the foreign power that's

supposed to be that's the subject of the surveillance, yes.

JUSTICE WINTER: What in your view could the government do if Yahoo was in Bern, Switzerland?

MR. ZWILLINGER: I think that would change the importance of the particularity requirement. I think the U.S. users, who use Yahoo's facilities in Bern, Switzerland --

JUSTICE WINTER: Suppose we have exactly the same number of -- the same people were using Yahoo --

MR. ZWILLINGER: Right.

JUSTICE WINTER: -- just that it's in Bern. How does that change the situation?

MR. ZWILLINGER: I think you follow -- I think the court in Bin Laden has it right in that respect, that is, if the foreign communications -- if the surveillance is taking place overseas, and it's a foreign communication facility, then I think the government has more freedom with the foreign intelligence exception to the warrant requirement to surveil that, because I don't agree that they fall under the exception when they're surveilling here, and I think the particularity doesn't need to be shown as dramatically to a U.S. court, because the consequences don't fall on U.S. persons.

JUSTICE WINTER: But the only U.S. persons affected by my hypothetical different from what we have in this case are Yahoo employees.

MR. ZWILLINGER: Oh, I see what you're saying.

JUSTICE WINTER: Yes.

MR. ZWILLINGER: If the same proportion of users --

JUSTICE WINTER: I'm saying, I mean -- I mean in the past we had the comfort of having technology and the targeted persons proximate to each other. Now, we -- we have a totally different technology. What difference does that make? What can the United States Government do -- in your view, what could it do if the -- if Yahoo's facilities were in Bern that it can't do now, because they're in Sunnyside?

MR. ZWILLINGER: Sunnyvale, California.

JUSTICE WINTER: Sunnyvale.

MR. ZWILLINGER: My answer is that we have always put more restrictions on the government operating on U.S. soil; and so, if the Yahoo system, if we're talking about a Yahoo system in -- operated by a Swiss entity, because I think the fact that Yahoo is a U.S. company matters to this. But if you're saying a Swiss entity is operating a communications facility that looks exactly like Yahoo in Switzerland does the government have to go to a U.S. FISA Court to show particularity, I would say the need for that would be less; that their surveillance of the Swiss facility would be more reasonable than it would be if they're operating on U.S. soil, because --

JUSTICE WINTER: I mean -- I mean, we used to live in circumstances where if people -- I had a civil case that involved long-distance phone calls in Japan from -- from Tokyo

to -- to Kobe, or whatever, and it was cheaper for those calls to be routed through Chicago than just routed in Japan.

Now, what difference does it make since the persons being -- actually being surveilled are on foreign soil? What difference does it make that the transmission facilities are -- are here or in Brazil or wherever --

MR. ZWILLINGER: I think the key question --

JUSTICE WINTER: -- constitutionally?

MR. ZWILLINGER: Yeah, I think constitutionally the key question is how does the lack of particularity harm U.S. persons, and -- and in this example, and, you know, I can spend as much time as you want on it, but -- but when you have an example like we have where more of our users are from the United States, the lack of particularity and getting the wrong account harms U.S. persons, and the jurisdiction --

JUSTICE WINTER: I guess what I'm getting at is shouldn't the Fourth Amendment focus on the targets, not the transmitters?

MR. ZWILLINGER: I think it focuses on both, because let me try another -- if there was a -- a hotel in the United States, and two foreigners were meeting, and they've chosen the United States as their choice of forum, and they went into a hotel room, and it was a foreign communication to a foreign communication, do we say the government can operate with impunity, warrantless basis to put a bug in that room, or do we

say that the fact that they're in a U.S. hotel matters that you can't surveil that room without process under U.S. law?

JUSTICE SELYA: No, we --

MR. ZWILLINGER: Jurisdiction matters.

JUSTICE SELYA: But we -- but we also say that if the government made a warrantless entry into that, into that room, that the hotel might not be able to challenge that, and it seems to me the transmission facility here is in a position of a hotel.

MR. ZWILLINGER: Except the transmission facility isn't passively -- if the government wants to barge into the hotel room and place a bug, that's different than the government coercing and under the power of the court compelling Yahoo to assist in what would be unconstitutional surveillance if a U.S. person were involved in that communication. If there were a U.S. person involved in that hotel room, the U.S. person using their facilities we would argue this is an unconstitutional interception, and we're asking -- and the government's asking us to participate in it. They're not picking the signals out of the air. They're saying Yahoo, under penalty of contempt, you must spend your time and energy intercepting [redacted] people [redacted] otherwise, we'll fine you. And I think that's different. We're coercing a U.S. company to comply with what we believe is an unlawful directive, and Congress told the Court to consider whether the directive is

lawful or not. I understand your point would there be standing, but this is not -- Yahoo's not suing. We're not looking to recover any money. We're not looking to exclude any evidence. I'm sorry.

JUSTICE SELYA: Let me move backwards, because I want to be sure I understand something. You keep talking about the -- the [redacted] errors that you've discovered in what the government in the -- in the accomplice that the government's saying.

Do I correctly understand that those [redacted] accounts are all accounts that were closed by the time you received your request to surveil those accounts?

MR. ZWILLINGER: I don't know that, that they were closed. We know they don't exist.

JUSTICE SELYA: Or they don't exist?

MR. ZWILLINGER: I don't know whether they ever existed and were closed or were closed for dormancy or were closed for termination. I just know they don't exist.

JUSTICE SELYA: All right. But it makes a substantial difference, doesn't it, because -- because it seems to me if the accounts -- if the accounts are merely accounts that have been closed that that -- that reduces greatly the possibility that they were errors at all. The government's information may be entirely accurate as simply that the parties may be -- may be one step ahead of the government and may have closed the

accounts. So it doesn't tell us very much.

MR. ZWILLINGER: Well, one --

JUSTICE SELYA: All we know is that the accounts no longer exist.

MR. ZWILLINGER: One step or seven, that is, at a certain point they get closed and get recycled and other people start using them. But, yes, I'm not here before you, and this wasn't the focus of the briefing to say [redacted] errors you must strike it down. I'm here to say look at the nature of the surveillance, look at the lack of particularity, look at how the names get on this list, that's important.

But the other thing that was responsive to a couple of your questions, and I don't want to let it go before my time is up, is the vesting of the entire discretion in the executive branch, because if this were two weeks ago, I would have stood before you, and I would have said, look at Keith, look at Katz, look at the warning about vesting the power in the branch that's interested in the outcome to make the important determinations, but this isn't two weeks ago. This is 2008, and the Supreme Court spoke last week in the Boumediene case; and the Boumediene case, while about habeas was really about reconciling privacy against security. And the question in Boumediene was is an executive branch only procedure of effective and reasonable substitute for the Constitutional guarantee of habeas; and the Court said it was not. And why

was it not an effective substitute? Because you cannot trust constitutional rights of this magnitude to a closed and accusatorial process that is run and determined by the interested party, who has an interest in the outcome just like the DNI in this case has an interest in the outcome. Keith and Katz taught us that the Fourth Amendment does not contemplate the Attorney General of the United States as a neutral and disinterested magistrate.

JUSTICE ARNOLD: I think it was important in the habeas case, the nature of the procedures that were actually available and promised were -- was important to the outcome in the habeas case; isn't that right, because the full panoply of judicial procedures wasn't really offered.

MR. ZWILLINGER: And that is my argument here. That is my argument here, that the full panoply of Fourth Amendment protections that are supposed to imbue to the benefit of U.S. persons are not here. They're not being given.

JUSTICE ARNOLD: I mean within -- I mean within the procedure itself. Here, they might be -- the decision with respect to whether those procedures have, in fact, been carried out may be -- may be entrusted to the executive branch, but I think it was important to the outcome in the habeas case the procedures themselves to whomever they might have been entrusted, for insufficiency.

MR. ZWILLINGER: Well, I'm going to stay with you here

though, because I do think the parallel remains. The procedures here, the PAA doesn't require the executive branch to do any of these things.

JUSTICE ARNOLD: No, but the record in this case indicates that the executive branch is doing quite a lot.

MR. ZWILLINGER: Well, I guess quite a lot depends on where you sit. They certainly are, according to the executive branch, are making a finding that the person -- the U.S. person, who's involved --

JUSTICE ARNOLD: You have agents. You have the directives.

MR. ZWILLINGER: The directives are for here for us to see. I would argue the directives say very little. The directives say --

JUSTICE ARNOLD: Do you have the executive order? Do you have the DoD procedures? They're not nothing, right?

MR. ZWILLINGER: They're not nothing, but they all go to the same point that there's a probable cause finding by the executive branch, not a particularity finding by the executive branch.

If I could reserve the rest of my time for rebuttal.

JUSTICE SELYA: Yes.

JUSTICE WINTER: We'll hear from the government.

MR. GARRE: Thank you, Judge Selya. May it please the Court, my name is Gregory Garre. I'm appearing here today on

behalf of the United States. As this Court recognized in the In re: Sealed case, the ability to reveal timely and accurate foreign intelligence information is vital to the nation's efforts to protect itself from foreign attack. The directives at issue in this case are an important crucial component of that ongoing effort.

If I could begin by addressing a number of the practical -- practical concerns that Mr. Zwillinger raised. First, with respect to the number of accounts covered by the tasking order. The vast majority of those accounts deal with non-U.S. persons outside the United States; and, therefore, no one, including Yahoo, as far as I understand from the briefs, is arguing that those accounts are subject to any Fourth Amendment consideration. There's only --

JUSTICE SELYA: What is the importance of that though, I mean, because the case is about the other accounts; isn't that right?

MR. GARRE: That's absolutely right.

JUSTICE SELYA: The FISA Courts -- the FISA Court, I think, referred two or three times to the fact that they assume that most of the vast majority of the people outside the United States are foreigners and not implicated, because the Fourth Amendment doesn't apply to them, but that's not really important to the case, is it?

MR. GARRE: Well, I think it puts the number that Mr.

Zwillinger gave into perspective, the [redacted].

JUSTICE SELYA: Right. But we're talking about those people only. I mean, those are the people whose rights are at stake here.

MR. GARRE: That's absolutely right, your Honor, and our argument focuses on that.

JUSTICE SELYA: Okay.

MR. GARRE: I mean, just briefly on the [redacted] number, as you mentioned, Judge Selya, it's true that accounts are opened and closed. [redacted] So the fact that accounts have been closed is not significant, and that's particularly true given that the large number of email accounts here is reflected by the fact that Yahoo is in noncompliance for several months. So, if you go back several months, it's not surprising that several accounts have been closed.

With respect to the protections against U.S. persons, who are not the targets of searches, there are ample protections in place to ensure that their communications are not intercepted.

First, there are the minimization procedures that exist under FISA and that have been applied for decades. The risk of incidental --

JUSTICE SELYA: That's post acquisition, isn't it?

MR. GARRE: That's post accusation, but it's post

acquisition in FISA, and it's important to understand the risk of incidental collection of U.S. communications from people, who are not targets of surveillance is the same in this case as it is in the typical FISA case; and so, we have a set of procedures that have been developed and applied and approved by the FISA Court for decades. And, your Honors, if you're interested in looking at those, I would point you to page 534 and 536, where they deal with the question of what happens when *communications from U.S. persons, who are not the subject of* targets are acquired. Those communications are disregarded under the procedures set forth at 534 to 536.

Second, if there is --

JUSTICE WINTER: Here, he suggested -- he stated that if those [redacted] numbers have been submitted to the FISA Court, if there was a provision for review by the FISA Court, those [redacted] would not have -- they would have been stricken from -- from the list.

MR. GARRE: Well, let me answer that question this way. The -- errors happen not infrequently under the FISA process as well where you get information that there is an account. It's presented to the FISA Court with similar information that the government looks at in determining whether to go up and account under the Protect America Act, and then it turns out that it's not the right account. So, the possible existence of error exists under FISA as it does here. You look

at the procedures in place to ensure that there is not an error, and I'm happy to address those.

First, let me just go back to the checks.

JUSTICE WINTER: Well, he did ask us to ask you how did these numbers get on this list. Maybe that's the point.

MR. GARRE: And the checks that are in place are these. And here I'm talking about any U.S. person, who is subject to surveillance outside the United States.

First, the Attorney General of the United States has to make a probable cause determination under Section 2.5 that the subject of surveillance is reasonably believed to be a foreign power or agent of foreign power. And the way that the Attorney General does that is first he gets a two -- a two- to three-page or lengthier letter from the director of the National Security Agency setting forth the facts and bases on which the government has to believe that this is a person, who is an agent foreign -- agent of a foreign power, for example, [redacted]

Next, the Department of Justice and National Security Division looks at that and through a careful back and forth process with the National Security Agency develops its own memorandum to the Attorney General, oftentimes a very lengthy memorandum, explaining the facts and circumstances that lead the government to conclude that this person is an agent of a foreign power. Then that information is submitted in an oral

briefing with high-level officials to the Attorney General, and there may be additional back and forth on the question of whether this person is a foreign agent. At that point, the Attorney General, as he did with respect to the U.S. persons in this case, would make a probable cause determination under Section 2.5 that the target is reasonably believed to be an agent of a foreign power. That's only the first part of the procedures in place. After that, you've got additional checks in place. You've got the targeting procedures that by statute were required to be approved by the FISA Court and that were approved by the FISA Court. I would direct your Honors' attention --

JUSTICE SELYA: Do any of those procedures go to Mr. Zwillinger called linkage?

MR. GARRE: Yes.

JUSTICE SELYA: [redacted] links up with that?

MR. GARRE: The targeting procedures require the government to ensure that the [redacted] an individual, whose outside the United States, and that is a particular linkage and a point your Honor is to, I believe, it's EA -- well, actually, the FISC Court discussed that at page 93 of its decision.

JUSTICE SELYA: But what linkage -- but even assuming that is used by the person outside the United States, who could

presumably could be a United States citizen, what then links that [redacted] with the -- the agent of a foreign power?

MR. GARRE: Well, I think -- oftentimes, this is sort of an academic question in the sense that oftentimes, and this is true under the FISA process, the government knows an individual by the [redacted] There is additional particularity findings that are made as part of the determination to [redacted] The government applies foreign intelligence factors, and those factors are discussed at page -- I believe EA 12 of the -- the ex parte joint appendix. Where there are particular factors that are approved at the time that a certification is approved by the Attorney General that limits the government's discretion in determining whether [redacted] will have foreign

intelligence information that is appropriately surveilled in the procedures that have been in place. So, in those two respects there are particularity findings with respect to each [redacted] that is subject to the balance.

I've talked about the 2.5 finding and the targeting procedures, which were approved by the FISC, and that part of the Court's decision is contained at EA 557. There are also the minimization procedures that were --

JUSTICE SELYA: Before you get to minimization, there's a suggestion in the petitioner's brief -- more than a suggestion -- that the fact that the procedures you've just described are aimed at the agent of a foreign power is itself unduly expansive, because that doesn't necessarily limit it. It's not necessarily self-limiting to someone whose interest are inimical to the United States, but could encompass, for example, [redacted] That phrase is simply too broad.

MR. GARRE: And I think as that -- that term is applied by -- by decades of practice, it rules out that hypothetical possibility.

JUSTICE SELYA: All right. So, in other words, the government views the agent of a foreign power used in this context as a term of art that has got a particular meaning in the foreign intelligence community?

MR. GARRE: Absolutely. And in particular, if the

Court has any doubts about this, we'd urge you to read the classified materials, including the director of national intelligence affidavit in support of our opposition to the stay motion, which -- which discussed the particular targets of the surveillance at issue in these case; and among those, including in particular, agents of international tourist -- terrorists organizations, which is a part of the definition of foreign agent, which is set forth in the FISA statute.

JUSTICE ARNOLD: What part of the legal apparatus that is relevant to this case uses the word "employee of foreign government" is that not -- is that in the Act?

MR. GARRE: I believe that's in the FISA Act in the definition of -- of foreign power, foreign agent. But this case is really an as applied constitutional challenge to the particular directives in here, but they haven't raised the facial constitutional challenge. The Court would determine the Constitutionality of the directives at issue in light of all of the procedures that had been applied and that are supported in the record and in light of the particular national security issue.

JUSTICE ARNOLD: I saw it. I think that's right, but I didn't notice that they called our attention to that portion of the statute.

MR. GARRE: I think that hypothetical possibility wouldn't render the statute facially unconstitutional, and it's

not before Your Honors.

With respect to the targeting procedures, too, I did want to make clear that if an error is detected, the procedures provide that the information acquired should be destroyed. There is no database that is acquired with information that is incidentally collected; and under the targeting procedures, there is a provision for destroying evidence, and that's at EA 19 and 53.

JUSTICE SELYA: Now, your brother counsel suggests that isn't true, for example, mistakenly collected information reveals evidence of a crime or other exceptions.

Are there exceptions?

MR. GARRE: All right. Your Honor, those -- those -- the answer to those questions appears at pages 534 to 536 of the classified appendix, but -- but to answer it more generally in this forum, incidental collections from U.S. persons is either destroyed -- there are procedures in place to make sure that it is destroyed and not used or disseminated. In -- in -- and that is -- that is the baseline procedures. The discussion of those procedures, as they play out in particular situations, I think, is illuminated at page 534 and 536. There is no database that is taken from incidental collections, and any -- the risk of incidental collections is the same here as it is under FISA.

There's another check on the errors, and I think that

this is important. There is a congressional reporting requirement where the executive has to report to the Congress by statute, semiannually, I believe, and this is in the Protect America Act, but the executive has undertaken by itself to provide reports to Congress every 30 days of any errors that have been detected in the regular analytical and technical checks of the surveillance that is being conducted. And that is an additional check. Of course, if -- if Congress is concerned that the program is not working, and not only can amend the statute, but to bring executive officials to it to explain what is going on, conduct hearings, and whatnot.

JUSTICE ARNOLD: I'm sorry to return to this point, but I just got on this court two to three days ago, so I'm trying to get up to speed here.

What exactly is the scope of the approval of the FISA Court to the government's procedures? What is the -- what is the -- what is the nature of the scope of FISA --

MR. GARRE: The FISA court, and this is in -- it's required in the Protect America Act. I believe it's Section 105(c)c, little C, the required -- the FISA Court was required to review the government's targeting procedures, and it was under a clearly erroneous monitor review.

JUSTICE ARNOLD: Target the procedures.

MR. GARRE: And the FISA Court's decision is produced in the materials that the Court has before it in the

classified --

JUSTICE ARNOLD: I've read it. I'm just -- I'm having difficulty -- okay. That's in the EA?

MR. GARRE: That's in the EA, that's right, your Honor.

JUSTICE ARNOLD: All right. Thank you.

MR. GARRE: So, you've got the probable cause finding, the targeting procedures, the minimization procedures. On top of that, you also have the requirement, the statutory requirement, that the Attorney General and the director of national intelligence find that significant purpose of the acquisition is to obtain foreign intelligence information. And here again, the executive has gone further, because they not only have made that finding at the certification stage, but they've qualified it in an important respect by establishing foreign intelligence factors that channel the discretion of the analysts, [redacted] and again those procedures are discussed at EA 12.

Let me talk a little bit about the location of the surveillance, because this was another emphasis of Mr. Zwillinger.

We think that the pertinent constitutional point is the only surveillance at issue in this case is surveillance by U.S. persons, who are outside the United States. That

surveillance is with respect to communications that are taking place that are initiated outside the United States; and in that respect, although it's true that e-mail is collected by Yahoo at the Sunnyvale, California office, that is no different than surveillance that has been conducted for decades outside of FISA with respect to satellite communications.

When FISA was enacted in 1978, the definition of electronic surveillance carved out radio communications, i.e., satellite communications, where one user is outside of the country; and so under FISA you've had for decades, and this is what the FISA Court said about this, on page 83 of its decision: "Without question Congress is -- Congress is aware and has been for quite some time that the intelligence community conducts electronic surveillance of U.S. persons abroad without seeking prior judicial authority." And one aspect of that is the satellite communications, where you have U.S. persons outside the United States communicating by satellite, and those messages are picked up at a satellite dish inside the United States. And for decades those communications have been outside the FISA process, and no one has argued that the warrant requirement applies to those communications. And that makes sense when you think about it, and I think it was Judge Whener, I think, who made this point that the focus ought to be on the targets themselves where the communications are taking place. If you had foreign to foreign email

communication, and most of the email communications --

JUSTICE WINTER: Not where the communications are taking place, whether people are communicating by --

MR. GARRE: Well, that's right. That's right, [redacted] I don't think anybody would argue that the Fourth Amendment would apply to that communication, even though the email communications go to account in Sunnyvale, California. I haven't understood Yahoo to argue that the Fourth Amendment would be implicated by that.

And, similarly, the Fourth Amendment isn't --

JUSTICE SELYA: You mean the interception there by you and Yahoo would not implicate the Fourth Amendment?

MR. GARRE: That certainly would be the government's view.

JUSTICE SELYA: I'm just making sure I'm getting your point.

MR. GARRE: Right. And similarly, I think that --

JUSTICE WINTER: It's not clear they're saying -- even if they're saying the Fourth Amendment wouldn't apply to that, it's not clear they're saying there should not be some judicial review of whether the underlying facts leading to the exemption

should not be -- shouldn't exist.

MR. GARRE: Well, as I understand their argument, they're not contesting that the vast majority of communications of non-U.S. persons outside the U.S. are not subject to the Fourth Amendment, so there is no prior judicial approval. With respect to the U.S. persons outside the United States, it's true, they're arguing that there should be prior judicial approval, and that argument is an argument that the warrant requirement applies to foreign intelligence surveillance.

JUSTICE WINTER: Well, not necessarily. You can cut the salami a little closer, because you can say that there has to be judicial review showing that they fall within -- that the U.S. persons are outside the United States and are foreign power agents with foreign power.

MR. GARRE: Well, I think, with respect, your Honor, I think we view the prior judicial approval requirement as tantamount to a warrant requirement. I think once you get outside the warrant requirement, and we think that this Court in the In re: sealed case recognize that there is a warrant exception to the foreign surveillance gathering, because this Court concluded that the search --

JUSTICE WINTER: Well, it wouldn't be a warrant in the traditional sense, because it would stop that location and relationship to a foreign power. That would be checked. The purpose of the surveillance, the nature of the surveillance

wouldn't be checked; and normally with a warrant, those would be checked.

MR. GARRE: And I think -- I mean, first of all, the executive and Congress, and this goes to the point that Mr. Zwillinger addressed. This isn't a case about the executives' conduct. This is a case about the executives' determination and Congress's determination. So this case fits within the category of the Youngstown analysis where the petitioner bears the heaviest burden to show that the executives, that the actions, the directives at issue are unconstitutional, because the executive is operating under a framework established by Congress and under a framework where the executive is reporting to Congress every 30 days on what it's doing.

Secondly, again, there have been for decades foreign surveillance intelligence gathering that takes place outside of any judicial approval of -- the FISA Court recognized that at page 83 of its decision. And the question is once you get outside of the warrant exception, which we think this Court recognized foreign surveillance intelligence is outside of in the In re: sealed case, then the question is reasonableness. Has the government reasonably balanced its interest and the information, and here all agree that the government has the highest order of interest in obtaining foreign intelligence information about the activities of our enemies.

JUSTICE ARNOLD: Of course, if you did have

independent review by the judicial branch that would contribute to a conclusion that what was going on was reasonable, would it not?

MR. GARRE: Sure.

JUSTICE ARNOLD: Outside of the warrant requirement?

MR. GARRE: That's true, it would be an additional factor. I've listed the -- we think very fulsome steps that the executive undertakes itself, you could -- certainly, you could add others, but it would come at a cost. It would come at a cost that Congress recognized and the executive recognized that the need for speed, secrecy, and flexible in obtaining foreign intelligence information is -- is great, is vital. I think the director of national intelligence has explained that in his classified declaration to this Court.

JUSTICE ARNOLD: The whole thrust of the development of Fourth Amendment law has sort of emphasized the watchdog function of the judiciary. If you just look at the Fourth Amendment, there's nothing in there that really says that a warrant is usually required. It doesn't say that at all, and the warrant clause is at the bottom end of the Fourth Amendment, and -- but that's the way -- that's the way it has been interpreted.

MR. GARRE: You're right, your Honor, but I mean I think it's important to recognize you do have judicial involvement insofar as you have the procedures being reviewed

by and approved by the FISA Court. You do have the involvement of other branches in that you have the legislative branch is required to receive reports. And then you have the executive branch undertaking this extensive process on its own. And we think, again, the factors, the probable cause determination, that this person is an agent of a foreign power, the targeting procedures that ensure that this person is outside, reasonably believed to be outside the United States when the intelligence surveillance goes up and remains outside the United States during the course of our surveillance.

JUSTICE ARNOLD: To put it bluntly, how does anybody know that it's going to happen?

MR. GARRE: Well, Congress knows, because the executive is reporting to Congress. The presumption is, and this presumption would apply in the Fourth Amendment context as well as any other constitutional conduct -- context, that the government, the executive acts constitutionally. There is a presumption of regularity. There's no reason certainly in the record of this Court to -- for this Court to believe that that presumption would not be appropriate here, and there are checks in place to ensure that the executive is acting appropriately under the statute, and in particular, the congressional reporting requirement.

JUSTICE ARNOLD: I don't mean to suggest that there's a presumption otherwise, but there is this development. There

is this long history and development of the Fourth Amendment, which essentially regards certain governmental action as deserving of scrutiny.

MR. GARRE: And we certainly appreciate that, your Honor, but I think to be -- to be frank, I think the extraordinary conclusion -- it would be an extraordinary conclusion for this Court to conclude that this foreign intelligence surveillance is subject to prior judicial approval when for decades it has been the case throughout our history that foreign intelligence surveillance with respect to U.S. persons outside the United States has been outside the -- conducted outside the requirement of any prior judicial approval.

JUSTICE ARNOLD: There's no Supreme Court case to that effect, is there?

MR. GARRE: I'm talking about the historical practice. You're right, there's been no Supreme Court case specifically addressed to this question. The Keith case reserved it.

JUSTICE ARNOLD: Reserved it expressly and rather presciently, I would think.

MR. GARRE: It did, your Honor, but again the Supreme Court said in the Dames & Moore case that historical practice is very important in interpreting the scope of constitutional provisions.

JUSTICE ARNOLD: There was a suggestion in the Bin

Laden case that surveillance of this kind is obviously not satellite, so something like that has been going on since the Civil War. There was a citation to a law review article to that effect. I don't know whether we can take judicial notice of that or not.

MR. GARRE: I think that's correct, your Honor. I mean I think certainly since the 1940s, electronic surveillance with respect to individuals outside the United States has taken place outside of the warrant requirement, and again the FISC Court found that.

JUSTICE WINTER: Couldn't much the same be said the day before Keith came down about the kinds of surveillance that was -- that went on there?

MR. GARRE: I'm not sure. I mean I don't think to the same breadth, your Honor. I don't think the same could be said, and I think -- I mean everyone acknowledges, and certainly --

JUSTICE WINTER: Certainly, every president, like election is, every president, who was called upon to address the situation asserted their right to conduct that, so which generally means it's being conducted.

MR. GARRE: That's true. I think everyone recognizes that where you're dealing with surveillance inside the United States, you are within the -- the, you know, heartland of Fourth Amendment protections; but at the same time, there is

long-standing precedent recognizing that when you're talking about communications outside the United States, even with respect to the U.S. individuals, you're getting far to the edge of that.

JUSTICE SELYA: Let me -- let me be clear in my own mind as to ask just what the government believes the issue is that is presented here, because I -- as I understand it, and let's for the time being set aside the -- the potential jurisdiction of standing issues. The government's principal case before us is that there is a national security exception that eliminates the necessity in this type of situation for a warrant requirement, and that the statute and the government's procedures under the statute, as exemplified in this case, comport with the other aspects of the Fourth Amendment that would be -- that would or might be adequate.

MR. GARRE: That's correct, your Honor. We haven't argued that we're exempt from the Fourth Amendment.

JUSTICE SELYA: That's exactly what I was getting at. That broad issue isn't presented in this case.

MR. GARRE: That's right, your Honor. And we've argued, and we've applied the standard to this Court framed in In re: sealed case to look to whether or not the FISA, as amended, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with

the protected rights of citizens; and through the multiple procedures that I've mentioned, which include the executive's own procedures and checks, as well as the congressional check of oversight, we believe that this is a reasonable response; and that this Court in the in re: sealed case viewed the government interest here as -- as on the highest order of magnitude; and obviously, in the wake of events of seven years ago, nobody including Yahoo disputes that. When you -- and this is a balancing. You have to look at the highest order of the government's interests. That is not determinative, but that's an important part of the balance. When you balance that against the procedures that are in place, procedures that are required to be approved by a FISA Court, specifically the targeting procedures, procedures that the executive has adopted, the 2.5 probable cause determination is not something that the executive created for purposes of trying to comply with the Protect America Act. This is a -- this is a determination that has been in place for decades and has been made by the Executive. It's a familiar determination made by the Attorney General based on facts, specific facts and circumstances gathered by the nation's top -- gathered by and passed by --

JUSTICE ARNOLD: Is there anything in the record about the history of the application of these procedures and the extent? Have they actually been used in the

circumstances -- in this circumstance?

MR. GARRE: The -- the executive order itself that establishes Section 2.5, and this is an order of the President. It was issued in 1981, and that is an order that has been followed. I don't think anyone disputes it's been followed, as to whether or not there's historical examples in the record. I don't know. I can tell you that it has been followed with respect to any surveillance of U.S. persons overseas for decades. It's an established --

JUSTICE ARNOLD: I think the track record would be an important aspect -- would be important in allowing us or anyone to decide the question of the likelihood of the application and conscientious application of the procedures, but apparently there's nothing in the record about that.

MR. GARRE: And maybe -- I may stand corrected on that by my colleagues; and if I do, I will let you know.

JUSTICE ARNOLD: Well, I think I haven't seen it.

MR. GARRE: Certainly, if the Court would appreciate a -- a discussion or explanation of the manner in which Section 2.5 has been carried out over the past few decades, as well as an example of the type of application that is made under 2.5, which is a very serious, very fulsome application, which specifically directed to the fact and circumstance that lead the government officials and ultimately the Attorney General to conclude that there is probable cause to believe

that this person is an agent of a foreign power, we would be happy to provide that to the Court.

JUSTICE ARNOLD: But your main point is that this wasn't just something hoped up for present purposes; it's been in effect for quite some time?

MR. GARRE: That's exactly right. That's exactly right. You have that process in place for decades, and you have these -- the minimization procedures in place which have been approved and used by the FISA Court in essentially the same form for decades. You have targeting procedures, which have been reviewed and approved by the FISA court, which are not only designed to ensure that the particular facility being used is reasonably believed to be outside the United States at all points in time during the surveillance at issue. But also provide that if a determination is made that that is no longer a case, the surveillance should cease, and that information improperly obtained should be destroyed.

In addition to that, you've got the significant purpose determination, which by statute the director of the national intelligence and the Attorney General must make to ensure that the significant purpose of the collection at issue is foreign intelligence information, and that is a key finding for purposes of taking this case outside of the warrant requirement that would apply to the typical Fourth Amendment case. And on top of that, you have the congressional oversight

responsibility by the statutes.

We would -- we think that this, this provision, these directives are in accordance with the -- of an act of Congress. They are in accordance with the best judgment of the government's top intelligence officials. They're in accordance with historical practice conducted in this nation with respect to foreign intelligence surveillance, and we would urge this Court to affirm the decision of the FISA Court.

Thank you very much.

JUSTICE ARNOLD: The petitioner has reserved rebuttal time.

MR. ZWILLINGER: Your Honors, there's a glaring hole in the Solicitor General's argument, and that relates to the [redacted] component here. The Solicitor General told you that when the person goes outside the United States that you can do surveillance on those communications that are sent from outside the United States, [redacted]

Let me go over that again. When the government asks us to turn over the information [redacted] let's take, for example, an employee of this -- someone here is being accused of participating in giving some information to a foreign power. When they're in

the U.S. and sending communications, FISA applies. As soon as they go outside the United States, the government [redacted]

[redacted]

[redacted]

[redacted]

You know, the Solicitor General talks about Congress spoke here, but to the extent Congress has spoken, then they turn around and admit they misspoke. And now they have a Senate report that says we failed to provide adequate protections for U.S. persons, and we are going to pass new legislation. They intentionally let the Protect America Act lapse. So to the extent congressional oversight even exists after February 16, 2008, which I'm not sure it does, it provides no check. Congress can't do anything differently. The statute has passed. The directives continue all the way until the expiration date, but the statute doesn't exist any more. It's not Congress's current view of how surveillance should be conducted.

I think that's an important point. Another important point though is the government relies on the long history of surveillance; and on that point, I recommend and commend the Court read the D.C. Circuit decision Zweibon, because in that decision, the Court says the history of warrantless surveillance before Katz is irrelevant. Until Katz and Berger came down, there was no holding from the Supreme Court that the Fourth Amendment applied to communications in surveillance in a wiretapping communication. So how can, under a different legal

regime, a long history of surveillance matter -- and Judge Winter, your point was exactly right in the Keith case, and this is especially discussed in the District Court opinion. The government made the same argument with regard to the long history of surveillance for domestic security. There is no separate traits or separate track. The executive claimed the authority to do a warrantless surveillance for both domestic security and foreign intelligence information, and the Keith Court rejected that long history.

I don't think I'm going to convince you now in the few minutes I have left that there shouldn't be a foreign intelligence exception to the warrant clause, but I would say Bin Laden took a close look at that and said that used to make sense. That used to make sense before Keith, and it used to make sense before FISA, and now it only really makes sense when the collection is overseas. So, going back to my example where [redacted] why is there a foreign intelligence information exception to the warrant clause [redacted] What are the circumstances that justify that? It's got to be different.

JUSTICE WINTER: Don't we have to know more about the number of U.S. persons in their circumstances that are, in

fact, the subject of these directives? [redacted]

MR. ZWILLINGER: It's a very good question, and the answer is I think the framework of the statute prevents anyone from ever knowing about that. In the sense that what the government said was very important. We know people by their email address. That's what he said. We know people by their email address. So, if an email address goes out to 40 people and says, while you're in Baghdad, here's some important information for you. All they know is the email address. So how could they apply any of their executive order certifications to determine that that person is a U.S. person, if all they know is their email address, and that's all they have to know, because the email itself says, I have reason to believe this person is out of the country. It says while you were in Baghdad, please do the following. Forty people are copied on that. When you asked the Solicitor General the question how people got on the list, he answered a different question, with all due respect to him. He answered the

question what do you do to protect U.S. persons you know are U.S. persons. He didn't answer the question what do you do when an email gets sent out to 40 email addresses that says while you are in Baghdad, do this. What do you do before you put them on the list. If all they know is it's an email address, I don't think we'll ever know how many U.S. persons are subject to surveillance, and that's one of the flaws.

The Solicitor General says we didn't make a facial challenge. All I can say to that is we said the directives were unlawful. The directives are issued under the Protect America Act. It's precisely because of the lack of particularity, the lack of prior review, the lack of information that none of these safeguards come into form. So, yes, we're saying the directives served on us are unlawful, but it does -- they're unlawful, because the Protect America Act that allows them violates the Fourth Amendment.

JUSTICE ARNOLD: The flaw, if any, would be in the directive, so...

MR. ZWILLINGER: The directives in the record say very little other than you will do what we say.

JUSTICE ARNOLD: And the sort of evident procedure.

MR. ZWILLINGER: Let me pose just one final observation. The Solicitor General made an important point. He said there is a presumption of regularity that attaches to executive branch action. My understanding of the law is the

law is, you know, a battle between competing presumptions, and the presumption of the Fourth Amendment is that the reason to etch over the Fourth Amendment is there isn't a presumption that the executive will always act in a constitutional matter, not when they're invading U.S. persons' right to be secure in their homes or their places or their papers, and the presumption that should apply here is that we cannot vest that discretion in the executive branch.

Thank you.

JUSTICE SELYA: Thank you, Counsel.

Thank you, all. We appreciate the arguments. We'll take the matter under advisement, including the motion to stay, which we have not ruled definitively. I also want to thank both counsel for the advocate and counsel for the government for driving us and coming to Providence for purposes of this hearing. At least we provided you with nice New England weather; and if you don't like it, stay for awhile.

We'll stand in recess.

THE CLERK: All rise.

The session of the Honorable United States Foreign Intelligence Surveillance Court of Review is now recessed. God save the United States of America and this Honorable Court.

(At 11:50 a.m., Court was adjourned.)

~~SECRET~~

CERTIFICATE

I, [redacted] RDR, CRR, do hereby certify that the foregoing transcript, consisting of 62 pages inclusive, is a true and accurate transcription of my stenographic notes taken on June 19, 2008, to the best of my skill, knowledge, and ability.

/s/ [redacted]

[redacted] RDR, CRR

Official Court Reporter

~~SECRET~~