

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/ISO
32 CFR 2003

SECRET

1 United States Foreign Intelligence Surveillance
2 Court of Review
3
4

5 In re: Directives to Yahoo, Inc.)
6 pursuant to Section 105B of the) Case No. 08-01
7 Foreign Intelligence Surveillance Act)
8
9

10 BEFORE: The Presiding Honorable Bruce M. Selya
11 Honorable Ralph K. Winter, Jr.
12 Honorable Morris S. Arnold
13
14

15 United States District Court
16 Courtroom No. 3
17 One Exchange Terrace
18 Providence, Rhode Island
19 June 19, 2008, 10:30 a.m.
20
21

22 [REDACTED] RDR, CRR
23 Official Court Reporter
24 United States District Court
25 595 Main Street, Room 514A
 Worcester, MA 01608-2093
[REDACTED]

Mechanical Steno - Transcript by Computer

SECRET

~~SECRET~~

2

1 Present:

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

5 Marc J. Zwillinger, Esquire
[REDACTED]

6 Jacob Summers, Law Clerk
[REDACTED]

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

~~SECRET~~

~~SECRET~~

3

I N D E X

	Page
1 Argument by:	
2 Marc J. Zwillinger, Esquire	4
3 Gregory G. Garre, Acting Solicitor General	32
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

~~SECRET~~

~~SECRET~~

4

1

PROCEEDINGS

2

3 THE CLERK: The Honorable Court. All rise.

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

9 You may be seated.

10 JUSTICE SELYA: Good morning.

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

14 Each side is allotted 45 minutes for argument.

15 JUSTICE SELYA: You may proceed, Counsel.

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

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

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

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

25 MR. ZWILLINGER: Obviously, this is a highly unusual

~~SECRET~~

~~SECRET~~

5

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

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

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

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

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

~~SECRET~~

~~SECRET~~

6

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

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

7 So what is your jurisdictional basis?

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

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

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

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

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

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

~~SECRET~~

~~SECRET~~

7

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

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

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

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

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

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

24 MR. ZWILLINGER: It does.

25 JUSTICE ARNOLD: Don't you get compensation?

~~SECRET~~

~~SECRET~~

8

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

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

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

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

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

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

~~SECRET~~

~~SECRET~~

9

1 injury.

2 JUSTICE ARNOLD: Would an injury give you standing?

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

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

11 MR. ZWILLINGER: Well, according to the government,

12 [REDACTED]
13 [REDACTED] but I would --

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

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

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

~~SECRET~~

~~SECRET~~

10

1 they mean that since [REDACTED]

2 [REDACTED]

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

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

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

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

~~SECRET~~

~~SECRET~~

11

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

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

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

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

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

~~SECRET~~

~~SECRET~~

12

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

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

15 JUSTICE WINTER: And what will such a user feel?

16 MR. ZWILLINGER: Because of the surreptitious nature
17 of the surveillance, they wouldn't feel anything. Their
18 accounts would be surveilled. Their private communications
19 would be disclosed. [REDACTED]

20 They would make their way on to some government list.

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

~~SECRET~~

~~SECRET~~

13

1 coincidence if by chance somebody would recognize it?

2 MR. ZWILLINGER: No, I don't think that's right,
3 because [REDACTED]

4 [REDACTED] and the communications themselves often
5 contain private revealing data about who is sending it; that
6 is, when you send an email, your signature is often at the
7 bottom of it.

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

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

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

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

~~SECRET~~

~~SECRET~~

14

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

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

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

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

~~SECRET~~

~~SECRET~~

15

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

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

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

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

25 MR. ZWILLINGER: I guess one response on the

~~SECRET~~

~~SECRET~~

16

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

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

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

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

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

~~SECRET~~

~~SECRET~~

17

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

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

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

~~SECRET~~

~~SECRET~~

18

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

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

20 MR. ZWILLINGER: All those --

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

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

~~SECRET~~

~~SECRET~~

19

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

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

~~SECRET~~

~~SECRET~~

20

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

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

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

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

~~SECRET~~

~~SECRET~~

21

1 MR. ZWILLINGER: If you could.

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

7 MR. ZWILLINGER: Right.

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

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

14 JUSTICE ARNOLD: And minimization?

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

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

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

~~SECRET~~

~~SECRET~~

22

1 So --

2 JUSTICE ARNOLD: Sitting at home not abroad?

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

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

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

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

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

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

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

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

~~SECRET~~

~~SECRET~~

23

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

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

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

~~SECRET~~

~~SECRET~~

24

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

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

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

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

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

~~SECRET~~

~~SECRET~~

25

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

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

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

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

9 MR. ZWILLINGER: Right.

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

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

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

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

~~SECRET~~

~~SECRET~~

26

1 JUSTICE WINTER: Yes.

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

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

10 MR. ZWILLINGER: Sunnyvale, California.

11 JUSTICE WINTER: Sunnyvale.

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

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

~~SECRET~~

~~SECRET~~

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

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

7 MR. ZWILLINGER: I think the key question --

8 JUSTICE WINTER: -- constitutionally?

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

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

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

~~SECRET~~

~~SECRET~~

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

3 JUSTICE SELYA: No, we --

4 MR. ZWILLINGER: Jurisdiction matters.

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

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

~~SECRET~~

~~SECRET~~

29

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

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

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

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

15 JUSTICE SELYA: Or they don't exist?

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

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

~~SECRET~~

~~SECRET~~

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

2 MR. ZWILLINGER: Well, one --

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

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

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

~~SECRET~~

~~SECRET~~

31

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

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

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

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

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

~~SECRET~~

~~SECRET~~

32

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

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

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

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

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

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

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

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

22 JUSTICE SELYA: Yes.

23 JUSTICE WINTER: We'll hear from the government.

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

~~SECRET~~

~~SECRET~~

33

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

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

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

18 MR. GARRE: That's absolutely right.

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

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

~~SECRET~~

~~SECRET~~

34

1 Zwillinger gave into perspective, the [REDACTED]

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

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

7 JUSTICE SELYA: Okay.

8 MR. GARRE: I mean, just briefly on the [REDACTED] number, as
9 you mentioned, Judge Selya, it's true that accounts are opened
10 and closed. [REDACTED]

11 [REDACTED] So the fact that accounts have been closed is not
12 significant, and that's particularly true given that the large
13 number of email accounts here is reflected by the fact that
14 Yahoo is in noncompliance for several months. So, if you go
15 back several months, it's not surprising that several accounts
16 have been closed.

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

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

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

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

~~SECRET~~

~~SECRET~~

35

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

12 Second, if there is --

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

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

~~SECRET~~

~~SECRET~~

36

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

3 First, let me just go back to the checks.

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

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

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

18 [REDACTED]

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

~~SECRET~~

SECRET

37

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

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

15 MR. GARRE: Yes.

16 JUSTICE SELYA: [REDACTED] links up with
17 that? ¶

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

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

SECRET

~~SECRET~~

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

3 MR. GARRE: Well, I think -- oftentimes, this is sort
4 of an academic question in the sense that oftentimes, and this
5 is true under the FISA process, the government knows an
6 individual by the [REDACTED]

7
8
9
10
11
12
13
14
15
16

17 [REDACTED] There is additional
18 particularity findings that are made as part of the
19 determination to [REDACTED] The
20 government applies foreign intelligence factors, and those
21 factors are discussed at page -- I believe EA 12 of the -- the
22 ex parte joint appendix. Where there are particular factors
23 that are approved at the time that a certification is approved
24 by the Attorney General that limits the government's discretion
25 in determining whether [REDACTED] will have foreign

~~SECRET~~

~~SECRET~~

39

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

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

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

17 [REDACTED] That phrase is simply too broad.

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

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

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

~~SECRET~~

~~SECRET~~

40

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

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

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

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

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

~~SECRET~~

~~SECRET~~

41

1 not before Your Honors.

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

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

12 Are there exceptions?

13 MR. GARRE: All right. Your Honor,
14 those -- those -- the answer to those questions appears at
15 pages 534 to 536 of the classified appendix, but -- but to
16 answer it more generally in this forum, incidental collections
17 from U.S. persons is either destroyed -- there are procedures
18 in place to make sure that it is destroyed and not used or
19 disseminated. In -- in -- and that is -- that is the baseline
20 procedures. The discussion of those procedures, as they play
21 out in particular situations, I think, is illuminated at page
22 534 and 536. There is no database that is taken from
23 incidental collections, and any -- the risk of incidental
24 collections is the same here as it is under FISA.

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

~~SECRET~~

~~SECRET~~

42

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

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

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

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

23 JUSTICE ARNOLD: Target the procedures.

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

~~SECRET~~

SECRET

43

1 classified --

2 JUSTICE ARNOLD: I've read it. I'm just -- I'm having
3 difficulty -- okay. That's in the EA?4 MR. GARRE: That's in the EA, that's right, your
5 Honor.

6 JUSTICE ARNOLD: All right. Thank you.

7 MR. GARRE: So, you've got the probable cause finding,
8 the targeting procedures, the minimization procedures. On top
9 of that, you also have the requirement, the statutory
10 requirement, that the Attorney General and the director of
11 national intelligence find that significant purpose of the
12 acquisition is to obtain foreign intelligence information. And
13 here again, the executive has gone further, because they not
14 only have made that finding at the certification stage, but
15 they've qualified it in an important respect by establishing
16 foreign intelligence factors that channel the discretion of the
17 analysts, [redacted]18 [redacted] and again those procedures are
19 discussed at EA 12.20 Let me talk a little bit about the location of the
21 surveillance, because this was another emphasis of Mr.
22 Zwillinger.23 We think that the pertinent constitutional point is
24 the only surveillance at issue in this case is surveillance by
25 U.S. persons, who are outside the United States. That**SECRET**

SECRET

44

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

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

SECRET

~~SECRET~~

45

1 communication, and most of the email communications --

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

4 MR. GARRE: Well, that's right. That's right, [redacted]

5 [redacted]

6 [redacted]

7 [redacted]

8 [redacted]

9 [redacted] I don't think anybody

10 would argue that the Fourth Amendment would apply to that
11 communication, even though the email communications go to
12 account in Sunnyvale, California. I haven't understood Yahoo
13 to argue that the Fourth Amendment would be implicated by that.

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

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

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

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

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

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

~~SECRET~~

~~SECRET~~

46

1 should not be -- shouldn't exist.

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

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

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

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

~~SECRET~~

~~SECRET~~

47

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

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

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

25 JUSTICE ARNOLD: Of course, if you did have

~~SECRET~~

~~SECRET~~

48

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

4 MR. GARRE: Sure.

5 JUSTICE ARNOLD: Outside of the warrant requirement?

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

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

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

~~SECRET~~

~~SECRET~~

49

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

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

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

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

~~SECRET~~

~~SECRET~~

50

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

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

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

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

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

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

25 JUSTICE ARNOLD: There was a suggestion in the Bin

~~SECRET~~

~~SECRET~~

51

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

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

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

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

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

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

~~SECRET~~

~~SECRET~~

52

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

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

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

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

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

~~SECRET~~

~~SECRET~~

53

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

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

~~SECRET~~

~~SECRET~~

54

1 circumstances -- in this circumstance?

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

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

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

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

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

~~SECRET~~

~~SECRET~~

55

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

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

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

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

~~SECRET~~

~~SECRET~~

56

1 responsibility by the statutes.

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

9 Thank you very much.

10 JUSTICE ARNOLD: The petitioner has reserved rebuttal
11 time.

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

18

19

20

21 Let me go over that again. When the government asks
22 us to turn over the information [REDACTED]

23 [REDACTED] let's take, for example, an employee of
24 this -- someone here is being accused of participating in
25 giving some information to a foreign power. When they're in

~~SECRET~~

~~SECRET~~

57

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

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

~~SECRET~~

~~SECRET~~

58

1

2

3

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

~~SECRET~~

~~SECRET~~

59

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

10 I don't think I'm going to convince you now in the few
11 minutes I have left that there shouldn't be a foreign
12 intelligence exception to the warrant clause, but I would say
13 Bin Laden took a close look at that and said that used to make
14 sense. That used to make sense before Keith, and it used to
15 make sense before FISA, and now it only really makes sense when
16 the collection is overseas. So, going back to my example where
17 [REDACTED]

18 [REDACTED] why is
19 there a foreign intelligence information exception to the
20 warrant clause [REDACTED]

21 [REDACTED]
22 What are the circumstances that justify that? It's got to be
23 different.

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

~~SECRET~~

SECRET

60

1 fact, the subject of these directives?

2 [REDACTED]

3

4

5

6

7

8

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

SECRET

~~SECRET~~

61

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

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

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

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

21 JUSTICE ARNOLD: And the sort of evident procedure.

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

~~SECRET~~

~~SECRET~~

62

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

9 Thank you.

10 JUSTICE SELYA: Thank you, Counsel.

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

18 We'll stand in recess.

19 THE CLERK: All rise.

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

23

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

25

~~SECRET~~

~~SECRET~~1 C E R T I F I C A T E
2
3

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

8
9

10

/s/

11

[REDACTED] RDR, CRR

12

Official Court Reporter

13
14
15
16
17
18
19
20
21
22
23
24
25~~SECRET~~