VAUGHN WALKER'S CHESS GAME: THE NEW RULES

The other day, I did a post that summarized where we are on the interlocking warrantless wiretap claims. I summarized the state of affairs as follows:

- Al-Haramain's briefing on summary judgment due in late summer with a hearing September 1
- The retroactive immunity challenge headed to the 9th for appeal, plus a possible refiling for telecom actions (probably) after January 7, 2007
- The hearing in Jewel scheduled for July 15
- The state cases dismissed pretty definitively
- The Jeppesen ruling and its potential effect on the government's invocation of state secrets in Jewell
- Any discovery action in the Seda case
- The legally required IG report on warrantless wiretapping due (ha!) next month

Since the beginning of the year, Walker has been proceeding very deliberately (read, slowly) with the cases under his control (indeed, the September 1 hearing date for al-Haramain may

suggest he continues to do so), during which time a number of issues in these cases have solidified. In some cases, this holds true just for his courtroom; in others, it holds true at the 9th Circuit. Most haven't been tested in SCOTUS yet. This deliberation sucks, insofar as the criminal statute of limitations on the primary illegal wiretapping that occurred in March 2004 has expired. But I think Walker allowed everything to mature such that—on Thursday—he felt he could move three of them forward at once. In this post, I'll explain what I think has matured in these cases, and look at how it affects the Jewel suit against the government. In a follow-up post I'm going to look at what it might mean for post-January 7, 2007 surveillance.

Here's my NAL understanding of what has matured in that time (as always, feel free to kick my ass on my misunderstanding of the law or any other aspect of this).

- The Court of Appeals made it clear that the government must assert state secrets with respect to individual pieces of evidence, not information. This means the government cannot—as it has tried to—just declare the entire question of whether US person data was vacuumed up a state secret.
- The Court of Appeals refused the government's interlocutory appeal of Walker's ruling that al-Haramain had sufficiently proved it had aggrieved status such that he could review the evidence to see

if the charity had been wiretapped (this was also an unsuccessful attempt to appeal his ruling that FISA trumped state secrets that they had flubbed the previous summer). This means the 9th is probably going to give Walker leeway to rule on other aggrieved party statuses, if he does so.

- Vaughn Walker got four new declarations presumably correcting an "inaccuracy" in how Bush's DOJ had described the surveillance done on al-Haramain and probably giving him a much better idea how the surveillance worked.
- Vaughn Walker just affirmed the government's insistence that the legislative record holds significant sway in these proceedings, but also that under *Navy v. Egan* Congress can legislate restrictions on the handling of classified information. This carves out a space where a judge can assess liability for illegal surveillance, even in the face of the government's attempt to claim this is all secret (though Walker's affirmation of this argument

hasn't been tested yet).
- The Supreme Court ruled in *Iqbal* that a plaintiff must submit specific facts for a claim to overcome qualified immunity of a government employee in his official duties.

What's Next

Now, if I understand this all correctly, it means that Walker will use the following process for suits going forward:

1. Is the suit prohibited by the FISA Amendments Act (that is, is it a state-based suit or a pre-January 7, 2007 suit against telecoms which the AG has certified should be dropped)?
2. If not, then the plaintiff should present a case for aggrieved status under FISA (and/or some other statute, which I'll get back to in my next post, maybe).
3. The government may only claim state secrets with regards to individual pieces of evidence, not information about the program generally, and if Walker finds the case to be sufficient, then the 9th isn't going to stop him from reviewing further

before ruling.
4. In addition to Walker's "FISA trumps state secrets" ruling (which still stands, but hasn't been tested in practice yet), even the government agrees the legislative record on the FAA can be reviewed closely to judge the law.
5. The plaintiff must overcome the bar set by *Iqbal*.

Now, granted, all of this doesn't get a plaintiff to Anthony Kennedy's doorstep (particularly not with regards to the FISA trumping state secrets in practice)—but it gets you part of the way there.

Not only does this seem to be the process in place, but Walker has indicated—at least preliminarily—that he thinks it offers real opportunity for plaintiffs to challenge the government on its warrantless wiretapping. In his retroactive immunity ruling, he wrote,

> The United States and the telecommunications company defendants counter that while suits against telecommunications companies are foreclosed, neither the statute nor the government's actions prevent plaintiffs from seeking redress for their constitutional claims against the government actors and entities. Doc #520 at 12. Lest any further reassurance be necessary, the SSCI report states: "The committee does not intend for [section 802] to apply to, or in any way affect, pending or future suits against the Government as to the legality of the President's program."
>
> The court agrees with the United States and the telecommunications company

> defendants on this point: plaintiffs retain a means of redressing the harms alleged in their complaints by proceeding against governmental actors and entities who are, after all, the primary actors in the alleged wiretapping activities. Indeed, the same plaintiffs who brought the Hepting v AT&T lawsuit (C 06-0672 VRW) are now actively prosecuting those claims in a separate suit filed in September 2008 against government defendants before the undersigned judge. Jewell v United States, C 08-4373 VRW, filed September 18, 2008. Jewell thus joins several other cases in this MDL which seek relief only against government defendants.

Walker here emphasizes Congress' insistence that claims against the government can move forward while asserting plaintiffs do have a means of redressing harm. He seems to have a reason to believe that—and not just in al-Haramain, but in Jewel, too. And that's coming from a guy who has read all the evidence submitted by EFF and all the declarations submitted by the government.

With that in mind, let's look at the Jewel suit, the suit against the government and government officials who illegally surveilled Americans that—Vaughn Walker says—offers a means to redress abuses. It alleges that the government and named defendants violated AT&T customers' First and Fourth Amendment rights, FISA, the Wiretap Act, the Electronic Communication Privacy Act, and the Administrative Procedures Act. Significantly, it focuses on the vacuuming up of data and data mining of it, rather than on the wiretapping that happened later. Thus, in the FISA, Wiretap, and ECPA violations, the complaint focuses as much on the use of illegally-collected information as its collection.

Now, Walker has explicitly noted that Jewel passes the bar set by FAA—it focuses on

government employees, and not the telecoms immunized by Congress.

The government has already invoked state secrets in this case. But—as I mentioned and EFF hammered on in their most recent filing—that invocation of state secrets claimed to protect about six kinds of information, not evidence. So at the very least, the government is going to be sent back to the drawing board to fight over state secrets on discrete bits of evidence, rather than on wide swaths of information. I suspect that will be the specific outcome of the hearing next month, perhaps in tandem with a more pointed direction to EFF to show aggrieved status.

EFF's Summary of Evidence

And there's a lot of evidence in question, most of which the government cannot possibly claim state secrets on. Back in October, EFF submitted a summary of evidence in the case, laying out its case that the government and the defendants violated the law (it was accompanied by several binders of the evidence itself). The narrative itself really is pretty comprehensive and I encourage you to read it for its content. But just in light of the government's attempt to claim state secrets, here are some of the pieces of evidence included in that summary.

Evidence implicating named individuals and showing the program violated FISA

- Presidential order authorizing the program (referenced in Lichtblau)
- SSCI testimony of Benjamin Powell (describing that surveillance was done pursuant to Presidential authorization)
- Jack Goldsmith's "blow through" FISA statement

implicating Addington
- 2007 SJC Ken Wainstein testimony (saying the written declarations did not constitute a proper written order)
- 2007 Background briefing with SAO (admitting the 4th Amendment covers call data)
- 2008 NGA George Bush speech (saying the telecoms had been told surveillance was legal)

General details about the program

- Michael Hayden confirmation hearing (for start date of program, many other details)
- Program reauthorization dates (Coffin statement to SJC)
- 2007 HPSCI hearing, Reyes statement (on what was collected)

Evidence on data mining and concerns about its legality

- 2008 DOJ IG Report on Alberto Gonzales' mishandling of information (including his notes on March 10, 2004 wiretap briefing describing legal problems with program)
- Yoo PBS Frontline interview (on FISA being inadequate, on computers plucking data

from emails and calls that might have intelligence value)

- 2007 Alberto Gonzales testimony (explaining why FISA was inadequate)
- 2007 HPSCI Mike McConnell testimony (explaining that original program was unlawful under FISA, describing data being put into database automatically, referring to billions of things going on, referring to pizza shop calls being minimized)
- 2006 interview of Chertoff admitting data mining
- Kathleen Turner letter to Reyes and Hoekstra (describing analysts "combing through" data)
- 2007 SJC Mike McConnell testimony (referring to database of collected data)
- 1982 DOD intelligence procedures (saying data is collected only after DOD employee receives information)
- Jack Goldsmith testimony
- Jim Comey testimony
- 2007 Tony Snow statement (saying the program did not change in 2007)
- 2007 Mike McConnell letter to Arlen Specter (on TSP

being a fake name invented to refer to wiretap part in 2006 to cordon off the data mining)
- Hayden testimony (showing his use of "conversation" and "communication" to hide extent of surveillance)
- US Attorney's Manual (on URLs as contents in some cases)

Evidence showing US person call data are vacuumed up and kept

- February 26, 2008 White House background briefing on FISA (admitting domestic calls are intercepted, but minimized)
- 2006 SJC Alberto Gonzales testimony (on information being kept indefinitely)
- James A Baker Frontline interview (admitting the program collects data from innocent people)
- 2006 Alberto Gonzales press release (referring to call data collection)
- 2006 Pat Roberts NPR interview (dismissing concerns about content by saying they collected call data—business records)
- 2006 Kit Bond PBS interview (describing the govt using what telephone number called

what other telephone number)
- 2006 Blitzer inerview with Bill Frist (confirming that call data from 10s of millions of Americans have been collected)
- Statements from 9 members of Congress acknowledging call data program
- Joseph Nacchio statements (about Qwest being asked to collect data)
- Verizon Vice President acknowledging that Administration asked for call records

Evidence regarding Jewel's San Francisco vacuuming of data and proof the Bay Area plaintiffs were affected by it

- Mark Klein declaration on Folsom street
- Scott Marcus declaration
- James Russell declaration (confirming accuracy of Klein's account)
- AT&T Wayne Watts delcaration to House Energy and Commerce (referencing surveillance pursuant to presidential power)

In addition to these official government unclassified sources, EFF referred to an abundance of journalistic work, the collected works of Eric Lichtblau and James Risen and Barton Gellman and Siobhan Gorman.

There are a few things missing (most critically, IMO, Jello Jay's letter to Cheney, a named

defendant, saying on the day before the Senate withdrew funding for data mining of this sort that the program reminded him of Poindexter~~Negroponte~~'s TIA; but also the October 23, 2001 Yoo memo eviscerating the 4th amendment, which we know they considered applicable to warrantless wiretapping). But EFF has cited repeated, unclassified admissions (many of them from the fight over immunity) that there was a data mining component based on large scale collection of data.

The Process

Now, clearly, the government is going to find it all but impossible to declare state secrets over most of this material. One obvious exception will be the Presidential orders to the telecoms. Another important possible exception is the material relating to the AT&T's San Francisco data gathering (though they have not prosecuted any of those who submitted declarations for leaking classified information, so it'll be hard there too). And perhaps not surprisingly, that same information—the San Francisco facility information—is the same information that plaintiffs will need to prove they're aggrieved parties (and note, one of these declarations is sealed, so we don't know what's in there). The question then becomes whether Walker will find that they have sufficiently proved they are aggrieved parties such that they get to the point where FISA trumps state secrets and that information can be considered in the suit. And also, whether or not Walker will apply his general understanding of the program, including what he has learned through al-Haramain, to his assessment of the *Jewel* plaintiffs' aggrieved status.

I don't know the answer to that—but Vaughn Walker did say that suing government employees provides recourse for plaintiffs. And remember, he has already seen the declarations submitted in *Jewel* as well as the four corrected declarations in al-Haramain.

If the suit gets that far, it'll be in roughly

the same position as al-Haramain is in right now, though rather than a specific document, the government will be asserting state secrets to prevent discovery on a range of evidence—regarding the San Francisco facilities, but also regarding how much of Americans' data gets swept up and how it is data mined to select targets for wiretapping.

That would hypothetically leave two related problems for the *Jewel* plaintiffs: getting beyond the immunity claims for government employees, and getting to the level of specificity required by *Iqbal*. Now, on *Iqbal*, I'm agnostic—the only four people about whom *Jewel* currently presents facts with any specificity are Bush, David Addington (assuming Goldsmith can serve as witness to Addington's desire to blow FISA away), Alberto Gonzales (who signed the March 11, 2004 authorization), and John Yoo (who is not named in the suit). This is where timing may play a critical role, however. If the IG Report comes out in time, it promises to describe:

> the involvement of the DoJ and the Federal Bureau of Investigation (FBI) in the Program, including the use of and control over Program information; compliance with relevant authorities governing the Program
>
> [snip]
>
> the evolution of the Presidential authorization as it affected NSA, the technical operation of the Program, the preparation and dissemination of the product of the Program, and communications with and representations made to private sector entities. The review will address access by NSA to legal reviews and information concerning the Program
>
> [snip]
>
> the involvement of the Office of the Secretary of Defense in the

> establishment and implementation of the Program

That is, we've been promised, in 35 days time and before the hearing on this, much more detail about the role of the individuals who implemented the program. I don't think we'll get it in timely fashion, but it has been promised.

But as for the immunity claims, this is where Walker seems to be insisting on the importance of the legislative record. In addition to his ruling that FISA trumps state secrets because there must be some kind of recourse for violations of FISA (the appeal of which, of course, the government flubbed), there's his repeated reference to the legislative record from FAA, which makes it clear that Congress at least claimed to believe the individuals who authorized the program could be sued. To some degree, Walker's ruling last week seems to have been a long statement saying, "you want me to read the legislative record on retroactive immunity strictly? then I'll read it attentively when it comes to suing George Bush, too."

The Laws

Ultimately, though, this suit may come down to the interpretation of what the laws in question mean. Here is the specific language EFF says the government violated. From FISA:

> A person is guilty of an offense if he intentionally— (1) engages in electronic surveillance under color of law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

From the Wiretap Act:

> (1) Except as otherwise specifically

> provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> [snip]
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> [snip]
>
> (2)(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with— (A) a court order directing such assistance signed by the authorizing judge, or(B) a certification in writing by a person specified in section 2518 (7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

From ECPA:

> (a) **Contents of Wire or Electronic Communications in Electronic Storage.—** A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> (b) **Contents of Wire or Electronic Communications in a Remote Computing Service.—** (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection— (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity— (i) uses an administrative subpoena authorized by a

> Federal or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title. (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service— (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
>
> (c) **Records Concerning Electronic Communication Service or Remote Computing Service.—** (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity— (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; (B) obtains a court order for such disclosure under subsection (d) of this section; (C) has the consent of the subscriber or customer to such disclosure; (D) submits a formal written request relevant to a law enforcement

> investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or (E) seeks information under paragraph (2). (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the— (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1). (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

EFF has a number of people saying this program bypassed FISA. Assuming the San Francisco materials are admissible, we have evidence that wire communications were intercepted and used—and at least for the period following March 11, 2004, any request of the telecoms to do so came with White House Counsel Alberto Gonzales' signature, after the Acting Attorney General had refused to sign off on it. But given the fact that they're doing data mining on meta-data, a lot of this will likely come down to the language of ECPA. As EFF makes clear in their

summary of evidence, the Administration has been playing games with the meaning of "content" and "communication" in its discussion of this program, and I guess the meaning of these terms with respect to emails is not settled.

Vaughn Walker has laid a lot of the ground work to get to assessing evidence in this case. But I’m not sure where the parsing on "communication" will go if we ever get to that stage.