# VAUGHN WALKER'S CHESS GAME: SUE THE TELECOMS PART ONE

In two earlier posts I laid out where Vaughn Walker seems to be going with the warrantless wiretapping cases. In this post, I'm going to consider his suggestion—made in his ruling rejecting a challenge to retroactive immunity—that the plaintiffs could sue the telecoms for activities after January 17, 2007 (note, Walker said January 7, but it's almost certain he meant January 17).

> Because, however, section 802's immunity provision may only be invoked with regard to suits arising from actions authorized by the president between September 11, 2001 and January 7, 2007, the dismissal is without prejudice. On May 15, 2009, plaintiffs submitted a "notice of new factual authorities in support of
> plaintiffs' opposition to motion of the United States" to dismiss. Doc #627. In the notice, plaintiffs cite news articles published in 2009 reporting post-FISAAA warrantless electronic surveillance activities by the NSA. Plaintiffs argue that these articles constitute "proof that the certification of former Attorney General Michael Mukasey that is the sole basis for the government's pending motion to dismiss is not supported by 'substantial evidence.'" Doc #627 at 3. The court disagrees. The court believes that the Attorney General has adequately and properly invoked section 802's immunity to the extent that the allegations of the master
> consolidated complaints turn on actions authorized by the president between September 11, 2001 and January 7, 2007.

> The court also believes, however, that plaintiffs are entitled to an opportunity to amend their complaints if they are able, under the ever-morestringent pleading standards applicable in federal courts (see, e g, Ashcroft v Iqbal, ___ US ___, 129 S Ct 1937 (2009)), to allege causes of action not affected by the Attorney General's successful invocation of section 802's immunity.

EFF had submitted the recent Lichtblau and Risen article in support of their argument that they could sue for past abuses, and in response, Walker said, "Well, why don't you sue for more recent abuses?"

Is Walker serious? Does he really think there is means to do that?

**The Recent History of the Wiretap Program and the Immunities**

Let's start by looking at the recent history of the mass wiretap program along with the immunities offered by Congress in 2007 and 2008.

**January 10, 2007:** FISA Court issues first order covering the program

**January 17, 2007:** Alberto Gonzales informs Congress FISA Court will now approve wiretap program

**May 2007:** FISA Court judge rejects Administration's order for a basket warrant

**May 15, 2007, 10 AM:** Jim Comey testifies before Senate Judiciary Committee, describes Hospital confrontation

**May 15, 2007, 10 AM:** US Intelligence meets to discuss collecting more intelligence in case of kidnapped soldiers in Iraq

**May 15, 2007, 12:53 PM:** US Intelligence decides to wiretap, debates "novel and complicated issues" relating to wiretap

**May 15, 2007, ~5 PM:** US Intelligence seeks Alberto Gonzales approval for basket warrant

**May 15, 2007, 7:38 PM:** Wiretap begins

**August 5, 2007:** Protect America Act becomes law; it authorizes:

> Sec. 105B. (a) Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine, based on the information provided to them, that—
>
> > (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act;
> >
> > (2) the acquisition does not constitute electronic surveillance;
> >
> > (3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they

> > are stored, or equipment that is being or may be used to transmit or store such communications;
>
> > (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
>
> > (5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).
>
> This determination shall be in the form of a written certification, under oath, supported as appropriate by affidavit of appropriate officials in the national security field occupying positions appointed by the President, by and with the consent of the Senate, or the Head of any Agency of the Intelligence Community, unless immediate action by the Government is required and time does not permit the preparation of a certification. In such a case, the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made.

It provides for this cooperation from telecoms:

> (e) With respect to an authorization of an acquisition under section 105B, the Director of National Intelligence and Attorney General may direct a person to—
>
> > (1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a

> > minimum of interference with the services that such person is providing to the target; and
>
> (2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.

It includes this immunity for telecoms:

> Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

**February 18, 2008:** PAA expires; orders under PAA may extend for one year

**July 10, 2008:** FISA Amendments Act becomes law; it authorizes:

> (a) Authorization- Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.
>
> (b) Limitations- An acquisition authorized under subsection (a)—
>
> > (1) may not intentionally target any person known at the time of

> > acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
>
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

It provides for this cooperation from telecoms:

> (h) Directives and Judicial Review of Directives-
>
> (1) AUTHORITY- With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to—
>
> (A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will

> protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
>
> (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

It includes this immunity for telecoms:

> (a) Requirement for Certification- Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the district court of the United States in which such action is pending that—
>
> > (1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;
> >
> > (2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;
> >
> > (3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55),

or 702(h) directing such assistance;

(4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was—

(A) in connection with an intelligence activity involving communications that was—

(i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and

(ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider

indicating that the activity was—

(i) authorized by the President; and

(ii) determined to be lawful; or

(5) the person did not provide the alleged assistance.

(b) Judicial Review-

(1) REVIEW OF CERTIFICATIONS- A certification under subsection (a) shall be given effect unless the court finds that such certification is not supported by substantial evidence provided to the court pursuant to this section.

(2) SUPPLEMENTAL MATERIALS- In its review of a certification under subsection (a), the court may examine the court order, certification, written request, or directive described in subsection (a) and any relevant court order, certification, written request, or directive submitted pursuant to subsection (d).

(c) Limitations on Disclosure- If the Attorney General files a declaration under section 1746 of title 28, United States Code, that disclosure of a certification made pursuant to subsection (a) or the supplemental materials provided pursuant to subsection (b) or (d) would harm the national security of the United States, the court shall—

> > (1) review such certification and the supplemental materials in camera and ex parte; and
>
> > (2) limit any public disclosure concerning such certification and the supplemental materials, including any public order following such in camera and ex parte review, to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification.
>
> (d) Role of the Parties- Any plaintiff or defendant in a civil action may submit any relevant court order, certification, written request, or directive to the district court referred to in subsection (a) for review and shall be permitted to participate in the briefing or argument of any legal issue in a judicial proceeding conducted pursuant to this section, but only to the extent that such participation does not require the disclosure of classified information to such party. To the extent that classified information is relevant to the proceeding or would be revealed in the determination of an issue, the court shall review such information in camera and ex parte, and shall issue any part of the court's written order that would reveal classified information in camera and ex parte and maintain such part under seal.

**How to Sue**

The timeline shows there are four different categories of activities for which the telecoms might be sued for this program:

- Surveillance that took place between January 17 and August 5, 2007 that violates FISA or ECPA (Note, Walker probably got the date wrong when he said EFF might sue for stuff after the retroactive immunity period ended on January 7, 2007—he almost certainly meant January 17 [corrected])
- Surveillance that took place between August 5, 2007 and July 10, 2008 that does not comply with PAA
- Surveillance that took place after July 10, 2008 that does not comply with FAA
- Surveillance that took place in one of the transition periods, particularly after PAA expired on February 18, 2008 but before FAA went into effect on July 10, 2008

**January 17, 2007 to August 5, 2007**

This is by far the most ripe period for suit for two reasons. First, this is a window in which telecoms have neither the retroactive immunity offered by FAA (which extends only to January 17, 2007) nor the immunity included in PAA and FAA for the activities authorized in those laws. Plus, we know there was a period around May 2007 in which the FISA Court did not immediately approve the basket warrant application submitted by the Bush Administration.

The key point to keep in mind, of course, is that a big chunk of the EFF suit against the telecoms pertains to Wiretap and Electronic

Communication Privacy Act violations, not just FISA (go here for the relevant excerpts of the law). So the big question for this period is how the government required the telecoms to vacuum and data mine call data? If Walker believes the vacuumed data constitutes "content," then ECPA might require the collection to be tied to a criminal investigation, which it would not be. If Walker believes the vacuumed data is simply meta-data, then it might be enough to have an administrative subpoena (but this would have to be reported to Congress). And I'm not sure it is clear, yet, whether the metadata from emails (which is a lot of what we're talking about) equates to metadata from phone calls.

In other words, the surveillance that took place after immunity expired but before PAA and FAA legalized the broader surveillance program may be subject to suit under ECPA.

**August 5, 2007 to July 10, 2008**

Let's build backwards from the immunity offered to telecoms to see whether there's any exposure to liability during the period covered by PAA, because the big question (it seems to me) is whether or not the purported focus on foreign intelligence leaves room for suit. The telecoms get immunity "for providing any information, facilities, or assistance in accordance with a directive under this section." "Any information, facilities, or assistance" is pretty broad and may well cover the data mining of US person data culled directly from the networks, particularly since the authorization itself extends to requiring telecoms to give, "all information, facilities, and assistance necessary to accomplish the acquisition." I'm betting the government would argue that they needed everyone's data to get the proper targeting of the ultimate targets of the wiretap.

The question, though, is whether or not restriction against electronic surveillance would moot that? Or whether the ultimate focus on foreign intelligence would lead Judge Walker to narrowly interpret the phrase "any

information, facilities, or assistance necessary to accomplish the acquisition?"

And it's actually worse than that. With FAA, Congress made the immunity for PAA surveillance even broader, described as, "any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007." Again, there's the question of whether the collection of US person data could be considered part of a directive under PAA that purportedly may target only foreign intelligence.

**July 10, 2008 to present**

The immunity for telecoms built into FAA is parallel to that under PAA—it extends immunity "for providing any information, facilities, or assistance in accordance with a directive under this section." There are just a few differences. First, the authorization in FAA more specifically prohibits the intentional targeting of US persons—though the use of "intentional" throughout is a pretty big loophole. And, more interestingly, the section requires surveillance "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." So there's the possibility of challenging telecom immunity because the surveillance did not comply with the Fourth Amendment. I'll explain why that might be important in a moment.

There's one other new wrinkle with FAA, one that applies to all three of these periods. In the clause that also gives the Attorney General instructions for certifying the telecoms to quality for retroactive immunity, FAA gives the AG instructions for certifying that telecoms qualify for immunity under PAA or FAA. The review process is the same—the same crappy ex parte review that Judge Walker just upheld last week.

With one difference.

For retroactive immunity, all Walker gets to review is whether the certifications given to

the telecoms said the activity was authorized by the President and was legal (whether or not it was, in fact, legal). Walker just gets to review whether the certifications say what they are reported to say.

But for other immunity certifications, it seems that Walker will be able to review the certifications for whether or not they are supported by "substantial evidence." That is, Walker appears to have more extensive means to review whether the certifications actually comply with FAA, PAA, the Wiretap Act, or 18 USC270(b), which reads:

> (b) **Required Certification.—** The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may— (1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> (2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made

> that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

This is an important difference from the retroactive immunity, it seems to me, because Walker has more leeway to actualy rule on the legal comprehensiveness of those certifications, and not just on whether the certifications say what we know them to say. Plus, this part of FAA means that the Administration can't invoke state secrets to prevent Walker's review.

Mind you, Walker couldn't actually tell us what he finds in his review, aside from whether or not he dismisses a suit. But again, that's better than where we are with al-Haramain, in which the government claims Walker can't even tell us whether the suit gets to go forward.

It's still Kafkaesque. But it's a better type of Kafkaesque.

I'm going to go ahead and post this, so the lawyers in the crowd can start telling me what a futile pursuit this would be. In the meantime, I'm going to do a last post on some reasons EFF might be able to make a claim.