FISA + EO 12333 + [REDACTED] PROCEDURES = NO FOURTH AMENDMENT

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Yesterday, I showed that the government claims it doesn't have a database of incidentally collected data from non-targeted US persons; and then I showed why that claim is not credible. Today, I'll point to another big loophole in the government's wiretapping program revealed by the FISCR opinion: the use of three or more different methods of getting around Fourth Amendment requirements of probable cause and particularity.

The opinion describes what it seems to present as abundant protections involved in the wiretapping at issue—noting that these protections are included not just in Protect America Act, but also Executive Order 12333 and certain classified procedures.

> Beginning in [redacted] 2007, the government issued directives to the petitioner commanding it to assist in warrantless surveillance [redacted, redacted footnote]. These directives were issued pursuant to certifications that purported to contain all the information required by PAA.
>
> The certifications **require certain protections above and beyond those**

> **specified by the PAA**. For example, they require the AG and the National Security Agency (NSA) to follow the **procedures set out under Executive Order 12333 2.5** …, before any surveillance is undertaken. Moreover, affidavits supporting the certifications spell out additional safeguards to be employed in effecting the acquisitions. This last set of **classified procedures** has not been included in the information transmitted to the petitioner. In essence, as implemented, the certifications permit surveillance conducted to obtain foreign intelligence for national security purposes when those surveillances are directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States. [my emphasis]

Much later, when the Court is testing the government's claim that certifications in question qualify as "reasonable," it again lists these several "safeguards."

> The government rejoins that the PAA, as applied here, constitutes reasonable government action. It emphasizes both the protections spelled out in PAA itself and those mandated under the certifications and directives. This matrix of safeguards comprises at least five components: targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, **procedures incorporated through Executive Order 12333 2.5, and [redacted] procedures [redacted] outlined in an affidavit supporting the certifications**. [my emphasis]

Understand—this opinion is not about whether PAA (or, more generally, a Congressionally-

sanctioned wiretap program) by itself authorizes under the Fourth Amendment the actions the government required the plaintiff to take. It is about whether PAA + EO 12333 (the Reagan Executive Order laying out our intelligence program, plus the amendments to that EO) + redacted procedures submitted in conjuction with, but not mandated by, PAA fulfill Fourth Amendment requirements. PAA, by itself, does not fulfill Fourth Amendment requirements.

FISCR uses EO 12333 to fulfill probable cause

Now consider why this is important. The opinion describes the role of EO 12333 in authorizing the wiretaps, using it to dismiss the plaintiff's probable cause concerns.

> The procedures incorporated through section 2.5 of Executive Order 12333, made applicable to the surveillances through the certifications and directives, serve to allay the probable cause concern. That section states in relevant part:
>
> > The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is **probable cause** to believe that the technique is directed against **a foreign power or an agent of a foreign power**.
>
> [citation omitted, emphasis original, link to EO added]. Thus, in order for the government to act upon the

> certifications, the AG first had to make a determination that probable cause existed to believe that the targeted person is a foreign power or an agent of a foreign power.

(Click through to read the further description on page 23 of what the AG gets from NSA to make this determination.) This strikes me as critically important. The FISCR is **not** relying on the following language—the language from PAA—to get to probable cause:

> 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. [my emphasis]

It is relying on **this** language, from EO 12333.

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided **that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power**.

In other words, probable cause here is not tied to the "reasonable belief" that the surveillance is directed at persons believed to be outside the US. It is not tied to the procedures used to come to that reasonable belief. Rather, probable cause requires solely that the technique is directed against an agent of a foreign power, and probable cause is specifically tied to techniques used within the US or **against a US**

person. The probable cause, here, is tied specifically to actions **and persons** within the US.

And we know that the AG certification that the surveillance "concerns" people outside the US (mandated by PAA) and the AG determination of "probable cause" (mandated by EO 12333) are different things, because the former remains good for one year, whereas the latter is based on an NSA statement limiting the surveillance to a shorter period of 90 days.

> [The AG determination is based on DOD regulations that] also required a statement of the period—**not to exceed 90 days**—during which the surveillance was thought to be required. [my emphasis]

So, one year for the certification tied to persons located outside the US, 90 days for the determination of probable cause related to agents of a foreign power that may or may not be located inside the US. (I'll explain why this 90 day limit is important in a later post, but for the moment remember that this opinion, which authorized ongoing wiretaps, was written on August 22, 2008, more than 90 days after PAA expired on February 16, 2008.)

And conveniently, PAA specifically allows for its use with other laws.

FISCR uses redacted procedures to fulfill particularity

But that's not all. Now we come to the matter of the redacted procedures, which is what the Court uses to dismiss concerns about particularity.

> The petitioner's arguments about particularity and prior judicial review are defeated **by the way in which the statute has been applied**. When combined with the PAA's other protections, the [redacted] procedures and the procedures incorporated through the Executive Order are constitutionally sufficient

> compensation for any encroachments.
>
> The [redacted] procedures [redacted] are delineated in an ex parte appendix filed by the government. They also are described, albeit with greater generality, in the government's brief. [redacted] Although **the PAA itself does not mandate a showing of particularity**, see 50 USC 1805b(b), this pre-surveillance procedure strikes us as **analogous to and in conformity** with the particularity showing contemplated by *Sealed Case*. [my emphasis]

And if all those redactions in this argument dismissing the need for particularity don't make you nervous, note there's an entire paragraph redacted following these two.

Review closely what this passage says. FISCR admits that it has, in *Sealed Case*, mandated something "analogous to and in conformity with" particularity. It acknowledges here that PAA does not itself mandate particularity at all. Only when PAA is applied in a certain way—with EO 12333 and with these redacted procedures—does the action the government is compelling the plaintiff to do overcome Fourth Amendment prohibitions on unreasonable search and seizure.

It's worth recalling, at this point, something Mary has pointed out: the FISCR is not here ruling on all activities conducted under PAA. It is only ruling on this particular order. That's because it **can't** rule that PAA itself is constitutional because—by itself—it is admittedly not. The determination of the constitutionality of the actions mandated under PAA can only be made in conjunction with a review of these redacted procedures.

And oh, by the way, the plaintiff doesn't get to see those procedures, at least not beyond the "greater generality" with which they're described in the government's brief.

> This last set of classified procedures has not been included in the information transmitted to the petitioner

And if the plaintiff got to see those redacted procedures, it would make all the difference. As Russ Feingold noted,

> **The decision placed the burden of proof on the company to identify problems related to the implementation of the law, information to which the company did not have access. The court upheld the constitutionality of the PAA, as applied, without the benefit of an effective adversarial process.** The court concluded that "[t]he record supports the government. Notwithstanding the parade of horribles trotted out by the petitioner, it has presented no evidence of any actual harm, any egregious risk of error, or any broad potential for abuse in the circumstances of the instant case." However, the company did not have access to all relevant information, including problems related to the implementation of the PAA. Senator Feingold, who has repeatedly raised concerns about the implementation of the PAA and its successor, the FISA Amendments Act ("FAA"), in classified communications with the Director of National Intelligence and the Attorney General, has stated that the court's analysis would have been fundamentally altered had the company had access to this information and been able to bring it before the court.

Now, Russ Feingold has read and been briefed on the unredacted opinion and has some idea what's included in those redacted procedures. And he says that if the plaintiff were given access to those redacted procedures so it could address the sufficiency (or not) of them with regards to particularity, then the Court would have ruled

the government's order unconstitutional.

It's a neat parlor trick the Bush Administration—with the full complicity of Congress—has pulled off. The FISCR all but admits that PAA, by itself, was unconstitutional. But it has allowed the government to use PAA to compel cooperation from telecoms, and then use AG determination (including, potentially, with regards to Americans claimed to be agents of a foreign power) and these redacted procedures (procedures which the telecom, which is virtually the only entity with standing to object to the orders, may not see, and procedures which are apparently not guided by any law) to get around the probable cause and particularity required by the Fourth Amendment.

The Fourth Amendment still exists, the FISCR maintains, but it exists somewhere you—and even the telecoms now required to spy on you—can't see.