FISA Amendments Act of 2008

Video Transcript

Prepared by the Office of General Counsel (OGC)
Formatting, Section Titles, and the Outline in the left margin added by ADET

11 November 2008
OVSC1203 Transcript filmed 11 November 2008

Introduction
Background
Carrier protection
History of FISA
Four kinds of electronic surveillance requiring FISC Orders
Evolution of Technology from 1978 to 2008
Probable cause is required for every FISC order

President's response – Terrorist Surveillance Program (TSP)
Communications providers were vulnerable
Congressional response – The Protect America Act of 2007
FAA changed only two things about FISA:
1. Electronic surveillance vs. non-US persons located outside of the United States
2. Conventional Collection vs. US persons outside of the United States requires a FISC order
What does FAA [702] do in terms you care about?
FAA Section 702 Certifications state:
Compell US Carriers – "Directives"
What else happens?
1. The court looks at procedures to establish ‘reasonable belief of foreignness’
2. The court looks at minimization procedures
3. The AG and DNI issue procedures to avoid reverse targeting
4. There is a lot of oversight

How is FAA Being Used?

Highlights of Targeting and Minimization Procedures:
Dissemination and Retention

Who to call for help

NSA 0030
I. Introduction

Hi! My name's [redacted] I'm from the NSA Office of General Counsel. The reason I'm here talking to you today, and the reason you are listening, is because there's been a big change in the federal law affecting electronic surveillance for foreign intelligence purposes. I will be going over some of the rules you'll need to follow as you engage in the activities covered by that law, but to start off with I'm going to have to give you a little background, hopefully, not a whole lot, and some of the stuff you have heard before. I'll tell you how we got to this point, because to understand where we are you have to understand how we got here.

II. Background

A. FISA legislation

1. FISA of 1978 — Regulates electronic surveillance for foreign intelligence purposes
2. FAA of 2008 — expires in 2012

B. Carrier protection

The FAA, the FISA Amendments Act also has a second part. I'm not going to talk about it much (because it doesn't apply to your day to day work) but you should know about it. It gave liability protection for US telecommunications companies as well as some technical changes to the old part of FISA. I won't go into any of that.
C. History of FISA
1. Congress initially regulated electronic surveillance for law enforcement.

2. There was no legislation regulating NSA and other Foreign intelligence Agencies.

D. Four kinds of electronic surveillance requiring FISC Orders.

- Radio or Wire
- Wire - one end in the United States
- Radio - where sender and all recipients in the United States
- Domestic radio communications

History of FISA

So where we started, FISA... Back in 1978, the very first time Congress acted to regulate electronic surveillance for foreign intelligence purposes - it was not acting in a vacuum. About 15 years before that (or so) Congress had regulated electronic surveillance for law enforcement purposes.

Giving the law enforcement folks a very strict set of rules and basically making almost any form of electronic surveillance done by the US Government unlawful except in accordance with a court order. We were left out of that. Foreign intelligence folks were left out of that because Congress thought that there was no need to similarly regulate what we did because we were not touching the private lives of US people very much.

After the Church and Pike Committees revealed that some of the things that NSA and other Foreign Intelligence organizations were doing did involve the private communications of US people more than Congress had thought - that's where FISA came from.

Four kinds of electronic surveillance requiring FISC Orders

And what Congress did in FISA was pick out four types of electronic surveillance. Four specific activities that they said you needed to go to court for before you can do them for foreign intelligence purposes. What were they? What are they? Since they didn't change, they are:

1. The collection of the radio or wire communication of US people who are inside the United States.

2. Second thing is the collection of wire communications inside the United States. And that has a technical definition; it means when you intercept a communication while it is traveling on a wire and has one end in the United States.

3. Domestic radio communications.

The only time you have to get a court order to collect radio communications (other than when you are targeting a specific US person in the United States) is when you're intentionally collecting a communication in which the sender and all intended recipients are physically located inside the United States.

So as long as we were targeting somebody outside the United States we didn't have to get a court order. If we made a mistake; if we accidentally targeted somebody inside the United States we would have to get a court order.

These four kinds of electronic surveillance are defined in the 1978 FISA in the definitions section, paragraphs F(1) to F(4).
intercepted a radio communication that was completely domestic, we weren’t in violation of the law, all we had to do was destroy it or get permission from the Attorney General (AG) to keep it … a very different regime than what was for the wire collection.

4. “Warrant-Worthy”

And the fourth category applied to other, what we call “warrant-worthy” collection in the United States. Anytime that the Intelligence Community (IC) was going to engage in a collection effort inside the United States, that a law enforcement entity would require a court order for, we have to get court orders under FISA.

So, the upshot of all of that, of those four types of electronic surveillance, really meant that for NSA, we had to go off and get court orders to target and we did that for about thirty years or so.

While it was sometimes cumbersome, sometimes a little complicated, as those of you who worked FISA know, it was manageable.

**Evolution of Technology from 1978 to 2008**

Things changed in a very big way after 9/11. All of the sudden we had a much different set of priorities than we had a day beforehand. And a lot had changed with regard to the way telecommunications were sent and received in relation to the thirty years or so since FISA had been enacted. In 2001, the United States had become the hub of the world’s electronic communications.

**Probable cause is required for every FISC order**

What we had to confront primarily going after the terrorists was that under FISA we had to have probable cause that every one of our targets was a foreign power or an agent of a foreign power.
H. The TSP.

President’s response – Terrorist Surveillance Program (TSP)

J. PAA – a Congressional response

Congressional response – The Protect America Act of 2007

They quickly enacted a law called the Protect America Act or PAA...which most of you have probably heard of...in 2007. It was done in a hurry, but Congress, while they felt the need to do something in a hurry, also wanted to have time to resolve the issue in a more comprehensive way. So they gave it a six month shelf life. That law, PAA, expired in February of 2008 and Congress then enacted the new law, the one you are here to hear about – the FISA Amendments Act (FAA).
III. FAA changed only two things about FISA:

A. Electronic Surveillance vs. non-US persons located outside of the United States

1. FAA left all FISA definitions as they were

2. FAA changed one exception to FISA

B. Electronic Surveillance vs. non-US persons located outside of the United States

2. Conventional Collection against US persons outside of the United States requires a FISC order

What does FAA [702] do in terms you care about?

So what does the FAA do in terms that you care about?
OK, FAA is a long statute. This is a copy of it, it's about 160 pages. I encourage you to read it, but I'll tell you it is not easy to understand, I am a lawyer, I've been doing this a while, and it's not easy for me to understand. The important things you need to take away from this are as follows:

**What FAA did, like PAA before it, was offer a means whereby the AG and DNI can authorize the targeting of people reasonably believed to be non-US persons outside of the United States, and they don't need individualized court orders to do so.** So, instead they have to make these certifications, these broad authorizations.

**FAA Section 702 Certifications state:**

What do these certifications have to include?

1. They have to certify that there are procedures in place to limit targeting to people reasonably believed to be outside the United States and the court has to review them.

2. FAA Section 702 Certifications must include (Cont'd.)
   a. Procedures in place to prevent the intentional acquisition of domestic communications
   b. Stated purpose of targeting must be to obtain foreign intelligence

3. Compel US Carriers – "Directives"

4. What else happens?
   a. Court looks at procedures to establish "reasonable belief that target is outside the United States"

   b. Court looks at minimization procedures in place to handle US person information that might be gathered

**Compel US Carriers – "Directives"**

So once these certifications are issued under section 702 of the statute (if you'd care to look at it), then the AG and DNI can authorize directives to US telecommunications companies compelling them to assist the US Government in gathering foreign intelligence.
What else happens?
So that’s the basics of it, what else happens?

1. The court looks at procedures to establish ‘reasonable belief of foreignness’
   - The court (I already said) gets to look at procedures for saying that there is a reasonable belief for saying that a target is outside of the United States. Once again - a major change from the targeting under FISA. Under FISA you had to have probable cause to believe that the target was a foreign power or agent of a foreign power. Here all you need is a reasonable belief that the target is outside of the United States.

2. The court looks at minimization procedures
   - The court has to look at the minimization procedures governing handling US person information gathered pursuant to the certification. Although court orders are not going to be issued for each individual target, the court is going to look at the procedures for handling the US person information that we are going to get and make a judgment that they are suitable for the targeting being done.

3. The AG and DNI issue procedures to avoid reverse targeting
   - The AG and DNI, another condition, they have to issue procedures governing reverse targeting in collection of domestic communications.

4. There is a lot of oversight
   - And lastly, there is a lot of oversight. Big surprise. The best place to look at what the oversight requirements are, are in what we call the “foreignness procedures” or the “targeting procedures” ...procedures whereby you define what it means to have a reasonable belief that somebody is outside of the United States. There are requirements for training.
and there will be some external looks by DOJ and DNI individuals.

How is FAA Being Used?

So, how is it being used? What is being done with FAA right now?
Highlights of Targeting and Minimization Procedures:
Dissemination and Retention

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36
Who to call for help

So, when you’re dealing with the issues that you’ll see on the test, when you’re dealing with real life, I anticipate and encourage you to call our office or the Office of Oversight and Compliance and ask questions. We get paid to worry about this primarily. If you have question anytime, day or night, no matter where you are,
NSOC...believe it or not...can find you a lawyer to answer your question. Take advantage of that.

That's probably the thing I want to leave you with. I wish you good luck and have fun with the FAA briefing materials after this.