# Chapter 22 – Programmatic Electronic Surveillance for Foreign Intelligence

## How does the use digital communications potentially subject domestic communications to international surveillance?

## What was the Bush II Terrorist Surveillance Program (TSP)?

## Letter from William E. Moschella

### This is a dense defense of the legal authorization for the TSP. You should unpack it and see if you accept the justification.

#### What does the letter argue that the president can do on his intrinsic constitutional authority?

#### What did In re Sealed Case say about this power?

#### What does *Katz* say?

#### How does the AUMF support the TSP?

#### What is the argument that the AUMF applies domestically?

#### How does *Hamdi* support this reading?

#### What is the precedent from WWI?

#### Why doesn’t the TSP require a FISA warrant?

#### What is the authorizing statute?

#### Which exception to the 4th Amendment might also shelter the TSP?

#### How would this be different from the checkpoint that was not allowed?

#### How was this program authorized? How does the reauthorization support the reasonableness argument?

#### Who was the TSP aimed at?

#### How do you think these people were identified?

#### What is data mining?

#### Does data mining require a 4th Amendment warrant?

#### Referring back to Chapter 21, what is the government’s track record in getting FISA warrants?

#### Why did the AG say the Bush administration did not get a FISA warrant for the TSP?

#### Why not use the FISA 72 hour grace period?

#### What did Office of White House Counsel (OLC) say about the TSP and the 4th Amendment?

#### Can you make an administrative search argument to support the TSP?

#### TSP was not reauthorized. How could the program be sheltered under FISA? Think about the FISA facilities provisions – could a FISC judge rule that the telcom switches in the US are FISA facilities and thus that the government can watch them with a single FISA warrant?

#### What about the traffic that does not concern terrorism?

### Al-Haramain Islamic Foundation v. Bush, 451 F. Supp. 2d 1215 (D. Or. 2006), rev’d, 507 F.3d 1190 (9th Cir. 2007)

#### How did plaintiffs originally get standing?

#### Why was standing ultimately denied?

### The standing problem – if no one can get standing because no one can prove they were listened in on, is there any other avenue for redress?

#### There are also federal criminal penalties – why are these unlikely?

#### Did Obama investigate the Bush II DOJ?

#### Why not?

### FISA Amendments Act (FAA)

#### How does this free the President from the need for individual FISA warrants for programmatic surveillance?

#### What does the court approve?

#### Does the court ever see the details of the plan?

#### What are the limits on judicial review?

## In re Directives [Redacted Text]\*, 551 F.3d 1004 (FISCR 2008)

### Who is challenging the surveillance directive?

#### What did the FISC rule?

#### Like all decisions since Matthews, this is a balancing decision – how does the court rate national security on one side of the scale?

#### What is the key word in establishing whether the FISA procedures meet the 4th Amendment?

#### What did Lincoln tell us about the constitution versus the nation?

#### What did the Court say about the claim that In re Sealed Case required that FISA procedures be the equivalent of a 4th Amendment warrant?

#### Do we know what procedures the court is reviewing?

#### What does the AG have to determine to use these procedures?

#### What did the DOD “regulations” require?

#### Who is the judge of those representations?

#### Does the court recognize the potential for error?

#### Does the court see that as a reason to require more 4th Amendment formality?

#### What is incidental collection of information?

#### Why does the court reject this as a problem?

#### Does the court, or anyone other than the Executive have the ability to verify these representations about the use of incidental information?

#### Thought question – given the rejection of the primary purpose doctrine, how could incidental information be converted into intelligence that would be retained?

#### What is the court’s conclusion about the reasonableness of the procedures?

### Notes

#### Determining the location of a person being electronically surveilled was easy when FISA was written.

##### How has this changed in the digital world?

##### Are packet systems tied to physical locations, i.e., does digital addressing unambiguously know where a packet came from? In thinking about this question, think about whether there are systems that can be used to confuse or mask the origin of digital traffic?

#### When these data streams are being analyzed, do you think that the system first determines if the traffic is from a proper foreign source as described in the protocol, and then looks at the data?

##### Can you get pattern information and still comply with minimization?

##### What was the caveat about minimization if you found evidence of criminal or national security import?

#### How much info can you get without triggering FISA or 4th amendment review?

##### What is the modern equivalent of pen registers?

##### What can you get from email headers and tweet addressing?

##### What about the servers that the information flows through?

##### If you tweet or call from your cell phone, what location information is available?

#### The FFA now applies FISA protections, such as they are, to US persons abroad.

##### How much protection is this?

#### What is a *Terry* stop?

##### Why are people objecting to these being used in NYC?

##### Should electronic surveillance be seen as a version of a *Terry* stop?

#### The FAA was argued this term in the United States Supreme Court.