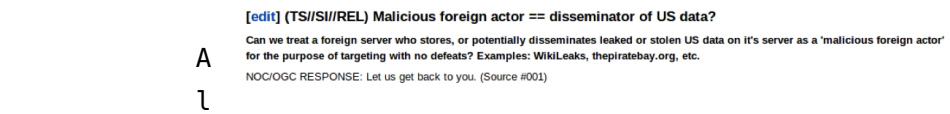
BETWEEN TWO ENDS OF THE WIKILEAKS INVESTIGATION: PARALLEL CONSTRUCTING THE FBI'S SECRET AUTHORITIES

Two pieces of news on the government's investigation of WikIleaks came out yesterday.

At the Intercept, Glenn Greenwald reported:

- In 2010, a "Manhunting Timeline" described efforts to get another country to prosecute what it called the "rogue" website
- In a targeting scenario dating to July 25, 2011, the US' Targeting and General Counsel personnel responded to a question about targeting WikiLeaks' or Pirate Bay's server by saying they'd have to get back to the questioner
- In 2012, GCHQ monitored WikiLeaks — including its US readers — to demonstrate the power of its ANTICRISIS GIRL initiative


[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

Also yesterday, Alexa O'Brien reported (and

contextualized with links back to her earlier extensive reporting):

- The grand jury investigation of WikiLeaks started at least as early as September 23, 2010
- On January 4, 2011 (21 days after the December 14, 201 administrative subpoena for Twitter records on Appelbaum and others), DOJ requested Jacob Appelbaum's Gmail records
- On April 15, 2011, DOJ requested Jacob Appelbaum's Sonic records

Now, as O'Brien lays out in her post, at various times during the investigation of WikiLeaks, it has been called a Computer Fraud and Abuse investigation, an Espionage investigation, and a terrorism investigation.

Which raises the question why, long after DOJ had deemed the WikiLeaks case a national security case that under either the terrorism or Espionage designation would grant them authority to use tools like National Security Letters, they were still using subpoenas that were getting challenged and noticed to Appelbaum? Why, if they were conducting an investigation that afforded them all the gagged orders they might want, were they issuing subpoenas that ultimately got challenged and exposed?

Before you answer "parallel construction," lets reconsider something I've been mulling since the very first Edward Snowden disclosure: the secret authority DOJ and FBI (and potentially other agencies) used to investigate not just WikiLeaks, but also WikiLeaks' supporters.

Back in June 2011, EPIC FOIAed DOJ and FBI (but

not NSA) for records relating to the government's investigation of WikiLeaks supporters.

> EPIC's FOIA asked for information designed to expose whether innocent readers and supporters of WikiLeaks had been swept up in the investigation. It asked for:
>
> > 1. *All records regarding any individuals **targeted for surveillance for support for or interest in** WikiLeaks;*
> > 2. *All records regarding **lists of names of individuals** who have demonstrated support for or interest in WikiLeaks;*
> > 3. *All records of any **agency communications** with Internet and social media companies including, but not limited to Facebook and Google, regarding **lists of individuals** who have*

> > *demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and*
> > 4. *All records of any* ***agency communications*** *with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding* ***lists of individuals*** *who have demonstrated, through monetary donations or other means, support or interest in WikiLeaks. [my emphasis]*

In their motion for summary judgment last February, DOJ said a lot of interesting things about the records-but-not-lists they might or might not have and generally subsumed the entire request under an ongoing investigation FOIA exemption.

Most interesting, however, is in also claiming that some statute prevented them from turning these records over to EPIC, they refused to

identify the statute they might have been using to investigate WikiLeaks' supporters.

> All three units at DOJ — as reflected in declarations from FBI's David Hardy, National Security Division's Mark Bradley, and Criminal Division's John Cunningham — claimed the files at issue were protected by statute.
>
> None named the statute in question. All three included some version of this statement, explaining they could only name the statute in their classified declarations.
>
> > The FBI has determined that an Exemption 3 statute applies and protects responsive information from the pending investigative files from disclosure. However, to disclose which statute or further discuss its application publicly would undermine interests protected by Exemption 7(A), as well as by the withholding statute. I have further discussed this exemption in my in camera, ex parte declaration, which is being submitted to the Court simultaneously with this declaration
>
> In fact, it appears the only reason that Cunningham submitted a sealed declaration was to explain his Exemption 3 invocation.
>
> And then, as if DOJ didn't trust the Court to keep sealed declarations secret, it added this plaintive request in the motion itself.
>
> > Defendants respectfully request that the Court not identify the Exemption 3 statute(s) at issue, or reveal any of the other

> > information provided in Defendants' ex parte and in camera submissions.
>
> DOJ refuses to reveal precisely what EPIC seems to be seeking: what kind of secret laws it is using to investigate innocent supporters of WikiLeaks.

Invoking a statutory exemption but **refusing** to identify the statute was, as far as I've been able to learn, unprecedented in FOIA litigation.

The case is still languishing at the DC District.

I suggested at the time that the statute in question was likely Section 215; I suspected at the time they refused to identify Section 215 because they didn't want to reveal what Edward Snowden revealed for them four months later: that the government uses Section 215 for bulk collection.

While they may well have used Section 215 (particularly to collect records, if they did collect them, from Visa, MasterCard, and PayPal — but note FBI, not NSA, would have wielded the Section 215 orders in that case), they couldn't have used the NSA phone dragnet to identify supporters unless they got the FISC to approve WikiLeaks as an associate of al Qaeda (update: Or got someone at NSA's OGC to claim there were reasons to believe WikiLeaks was associated with al Qaeda). They could, however, have used Section 215 to create their own little mini WikiLeaks dragnet.

For the same reason, they could not have used the PR/TT-authorized Internet dragnet to identify those who might have communicated with Assange or Bradley Manning Support Group members (though by this point they already had David House's computer with a membership list of the latter on it). The domestic Internet dragnet was operational, after having been shut down already, between at least October 2010 until the

end of 2011. But it, like the Section 215 dragnet, was apparently limited to terrorist identifiers.

Finally, we know under Special Procedures (SPCMA) approved in 2008 and piloted in 2009, NSA claimed the authority to track which Americans were in contact with foreign targets like Julian Assange, using communications data collected somewhere offshore. Significantly, there is no restriction to terrorism uses for SPCMA; analysts need only cite a foreign intelligence purpose. In an Espionage investigation of WikiLeaks after the adoption of SPCMA, all US person metadata collected internationally off the WikiLeaks server would have been fair game (though NSA would have to comply with dissemination limitations).

There is no authority permitting this SPCMA collection. NSA and DOD and DOJ simply claimed it under Article II. If that's what they're using to investigate WikiLeaks' supporters, I can imagine why DOJ wouldn't want to reveal that in a public filing in a FOIA case!

Particularly given the way at least two providers challenged either the gags or these criminal subpoenas themselves, there is zero reason to believe DOJ was doing anything other than providing some other claimed source for the evidence they wanted to submit to the grand jury (though there are some interesting NSLs that got challenged by various service providers in that same 2011 time frame, including the presumed Credo one).

So there are 3 details about the US investigation into WikiLeaks during 2011 of interest:

- By June 2011, they were using an authority to conduct such an investigation that they refuse to disclose
- They were, through that very

same period, issuing criminal subpoenas that providers were challenging
- NSA refused to say, in writing and after that EPIC FOIA was filed, whether analysts could incidentally collect US person communications to the WikiLeaks server based on a claim it was a malicious actor

Given all that the government has declassified — including references to SPCMA — I wonder if DOJ would now be willing to tell EPIC what statute — or lack thereof — it is hiding behind.

Updated: Changed reference to O'Brien's reporting because it said the opposite of what I intended to say.