THE FBI'S TWO WEEKS OF PEDDLING KIDDIE PORN AND SECTION 702

As you may have heard, from February 20 to March 4, 2015, the FBI was operating the world's largest kiddie porn site, during which point it hacked the site and thereby IDed the IP address of up to 1,500 users, both in the US and abroad.

Ars reported on the first known bust here and Motherboard's Joseph Cox was one of the first to report on the scope of this enforcement action.

> A new bulletin board site on the dark web was launched in August 2014, on which users could sign up and then upload whatever images they wanted. According to court documents, the site's primary purpose was "the advertisement and distribution of child pornography." Documents in another case would later confirm that the site was called "Playpen."
>
> Just a month after launch, Playpen had nearly 60,000 member accounts. By the following year, this number had ballooned to almost 215,000, with over 117,000 total posts, and an average of 11,000 unique visitors each week. Many of those posts, according to FBI testimony, contained some of the most extreme child abuse imagery one could imagine, and others included advice on how sexual abusers could avoid detection online.
>
> An FBI complaint described the site as "the largest remaining known child pornography hidden service in the world."
>
> A month before this peak, in February 2015, the computer server running Playpen was seized by law enforcement

> from a web host in Lenoir, North Carolina, according to a complaint filed against Peter Ferrell, one of the accused in New York. (Data hosts in Lenoir contacted by Motherboard declined to comment. One of them, CentriLogic, wrote "We have no comment on the matter referenced by you. Our obligations to customers and law enforcement preclude us from responding to your inquiry.")
>
> But after Playpen was seized, it wasn't immediately closed down, unlike previous dark web sites that have been shuttered by law enforcement. Instead, the FBI ran Playpen from its own servers in Newington, Virginia, from February 20 to March 4, reads a complaint filed against a defendant in Utah. During this time, the FBI deployed what is known as a network investigative technique (NIT), the agency's term for a hacking tool.

The other day, the judge in one of these cases, Robert Bryan, ruled that he wasn't all that bugged by FBI running the world's largest kiddie porn site for almost two weeks. The NYT has posted a "room for debate" op-ed weighing whether it is ethical for the FBI to run a kiddie porn site.

I've got an entirely different question, though one that may affect the ethics of the question. Why did the government have to take over the site itself in the first place? Why couldn't it have hacked the site while it was still being hosted by a web host in Lenoir, NC?

Which has me wondering whether the FBI's operation of the world's largest porn site was an effort to hide the earlier parts of this investigation, and the authorities it used.

The evidence against the men in the cases I've reviewed consists of three things: the IP addressed identified in the period when the FBI operated the site, sometimes physical evidence

from a search of their home, and log files and other activity information going back to the period when the website was first set up, in August 2014.

While some of those log files might have been available when the FBI took the site over, it may not have been. Still, the FBI could have gotten those files with a subpoena from the earlier period, once they identified where the site was hosted.

Still, I'm struck by the timing of the sites existence, starting in August 2014, with FBI taking it over in February 2015.

That happens to coincide interestingly with two interesting dates in the life of Section 702. On August 24, 2014, Thomas Hogan approved an expansion of Section 702 minimization procedures to permit the sharing of Section 702 obtained information with the National Center for Missing and Exploited Children.

> Hogan approved a change to the FBI minimization procedures that permitted dissemination of 702-collected information to the National Center for Missing and Exploited Children if it is "evidence of a crime related to child exploitation material, including child pornography," or for the purpose of obtaining technical assistance (the NCMEC keeps databases of images of child porn to track when new images are released).

And on February 4, 2015, Bob Litt revealed in a speech the list of crimes for which the government could use Section 702 derived information to prosecute (and he did so, seemingly, to correct comments he had made the day before that such a list had not been approved).

> [T]he government will use information acquired under Section 702 as evidence in a criminal case only in cases related

> to national security or for certain other enumerated serious crimes, and only when the Attorney General approves. And in that respect I just want to note that this morning's press reports that the Director of National Intelligence's General Counsel told reporters yesterday that we hadn't devised the list of crimes yet. The General Counsel for the Director of National Intelligence forgot that in fact we had. And so today I want to say that in fact the list of crimes other than national security crimes for which we can use Section 702 information about U.S. persons is crimes involving death, kidnapping, substantial bodily harm, conduct that is a specified offense against a minor as defined in a particular statute, incapacitation or destruction of critical infrastructure, cyber security, transnational crimes, or human trafficking.

Kiddie porn was, unsurprisingly, in that list.

Mind you, none of the defendants in this case have gotten any notice that Section 702 was used against them. But there are many conceivable ways it might have been, particularly given that, because it operated on Tor, would not have been identifiable, at first, as a US person site (and in any case, could have been "targeted" at other users on the site).

So the coincidence on the timing — with the minimization procedures changed just as the site opened up in 2014, and the authorization to use for prosecution of US persons made public just before FBI took over the site — does raise questions for me. One of which is this: did the FBI take over the server, rather than deploy the hack on it while it was running in North Carolina, to ensure that these 1,500 users wouldn't get FISA notices?