Written by **C. Mitchell Shaw** on March 25, 2017

In Child Pornography Case, Government Admits CIA Leaks Are Real

The fallout from the CIA hacking program — made public by WikiLeaks just over two weeks ago — just took a strange turn. In a case involving charges of child pornography, the federal government as good as admitted that the leaks contained in Vault 7 are genuine.

The case goes back to 2015 when the FBI operated a child pornography website for two weeks. Yes, you read that right. From February 20 to March 4, 2015, the FBI ran a website with more than 23,000 actual pictures and videos of children being sexually abused, including more than 9,000 of which could be downloaded by visitors to the site. According to court records, some of those children were almost too young to be in kindergarten.

It began when the FBI discovered the location of the server for the so-called Playpen website, which was accessible only via the Tor network. The FBI raided the location, arrested the operator, and made the decision to leave the website up and running and allow visitors to the site to continue downloading images and videos. The FBI's reasoning (if it can rightly be called that) was that federal agents had the ability to inject malware into the server that would work its way back to the users' computers, defeating Tor's anonymity all along the way. The FBI tracked the site's visitors and later made more than 135 arrests including "a pediatrician, a math teacher, a professor, a public school administrator, a preschool teacher, a former bank executive and a federal drug enforcement agent," according to a report from deepdotweb.com. Somehow, in the darkened mind of the FBI, the arrests justified spending two weeks peddling child pornography. And this is at least the third time the FBI has done this type of thing.

But then, this is the same FBI that helped the NSA give us Fast and Furious.

If the desire is to arrest and prosecute those who frequent child pornography sites, one might reasonably expect the agency to press on — even in the face of legal challenges — to get those convictions, right? Well, that all depends.

When the lawyer representing Jay Michaud, a school administrator from Vancouver, Washington, challenged the government's case against his client, demanding to see the source code for the hack the FBI alleges led agents to his client, the government dropped the case. According to a report by ZDNet from March 6:

> The FBI used a "network investigative technique" — a hacking tool that in any other hands than the feds would be considered malware — to deanonymize the users of the Tor browser, a widely used app for easy access to the dark web, during its 2015 investigation into the website.

> Little is known about the hacking tool, but it was known to be able to gather real-world information on Playpen visitors, such as IP addresses — details of which should have been protected by Tor.
>
> But the government refused to reveal the full source code of the exploit in court, and so the judge tossed out the evidence, rendering a significant set-back to the government's case.

The government then dropped its case but is "asking the case to be reopened once the exploit is no longer classified." Let that sink in. The government used a tool it refuses to divulge, but wanted the "fruit of the secret tree" to be admissible as evidence. When that failed, the government that knowingly — *willingly* — hosted a website rife with the types of pictures and videos that make up the darkest nightmares any decent person could imagine, simply called a Mulligan and walked away — hoping to come back later and try again.

And Motherboard is reporting that in a recent court filing, Colin Fieman, a federal public defender in Washington, wanted to admit some of the WikiLeaks disclosures from Vault 7 as evidence in the case against his client who was charged in the Playpen case. Fieman wanted to show that — because of the hacking tools the CIA developed (and lost control of) — it would be impossible for even a computer forensic expert to show whether someone using the CIA's cyberweapons planted the child pornography on his client's computer.

The documents and files Fieman wanted to introduce are those that are — thanks to WikiLeaks — widely available on the Internet. As District Judge Robert Bryan wrote in his court filing, those documents and files may show that the government possesses "the ability to hack into a computer without leaving any trace."

In fact, in an article about those cyberweapons, this writer recently observed:

> Since the hackers would then have remote access control over any such device, all files and folders would be available to the hacker. Worse yet, having control of the device would also allow the hacker to either remove or add files and folders. If the hacker wanted to bring an adversary down, it would be a simple matter to create a hidden folder containing illegal files — including child pornography — on the victim's device to be "discovered" at a later date by investigators serving a warrant. Such a sting operation would look — for all the world — like a legitimate law-enforcement activity. Even if it did not end in a prosecution and prison, the victim could be branded for life. After all, this is almost exactly what happened to former CBS News correspondent Sharyl Attkisson. In her case, the hidden files that were secretly placed on her computer were classified government documents for which Atkisson could have been charged under the Espionage Act for possessing.

As a direct result of the government creating tools capable of that, the new reality is that anyone accused of possessing any type of illegal computer file — even child pornography — has a much greater benefit of the doubt now than ever before. In fact, in the absence of a confession, this writer would — if serving on a jury — vote not guilty in such a case.

As it stands though, the government — again — gets to have it both ways. In the case in Washington, the government lawyers were able to keep the Vault 7 materials from being admitted as exhibits. Their argument? The files are "classified." Never mind that they are publicly available to anyone with Internet access. Never mind that they show exactly what Fieman asserts they show. They are "classified" and cannot be admitted.

This is the clearest admission of the validity of these documents and files so far. This writer noted in a previous article that the CIA had as much as admitted their validity:

> And the CIA published a statement Wednesday [March 8] that began by stating that the agency has "no comment on the authenticity of purported intelligence documents released by Wikileaks or on the status of any investigation into the source of the documents." The statement then went on to defend the agency's efforts to "aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other adversaries." While neither explicitly confirming nor denying the validity of the "purported" documents and files, the statement condemns WikiLeaks' disclosure of the information, saying that it is "designed to damage the Intelligence Community's ability to protect America against terrorists and other adversaries." The statement added, "Such disclosures not only jeopardize U.S. personnel and operations, but also equip our adversaries with tools and information to do us harm."
>
> Let's unpack that just a bit, because it says more than the CIA likely intended to say.
>
> If — as the CIA would have the American public believe — the authenticity of the leaked documents and files is questionable, how could their disclosure possibly "jeopardize U.S. personnel and operations" or "equip our adversaries with tools and information to do us harm"? Add to that the germane fact that — in a departure from previous leaks published by WikiLeaks — the whistleblower organization chose to redact the documents and files before publishing them on its website for the express purpose of keeping those tools and that information from harming anyone. The software tools (read: cyber weapons) WikiLeaks reported on were not released to any and all, but were made available only to the manufacturers of hardware and software affected by those "tools," so that the manufacturers could develop and release security patches to nullify the effectiveness of those weapons.
>
> The CIA — in an attempt to demonize WikiLeaks — has, by its own words, admitted that the disclosures are genuine. But that is what happens when — after being caught developing tools to turn computers, mobile devices, televisions, and other electronic devices against their users — the agency then attempts to duck and cover by talking out of both sides of its face.

Now, with government lawyers arguing — and a judge agreeing — that the documents and files are classified, there can be no question of their validity. If they are not real, they are not classified. Since the government admits they are classified, they must be real.

Since the evidence is becoming clearer that the intelligence community is a pack of gun-running, child pornography-pedaling, computer-hacking, pathological liars, is there one good reason to keep them around?