



**HOUSTON★CHRONICLE**  
 As low as \$1 per week / Unlimited Digital Access  
 HoustonChronicle.com | App for iPhone and iPad | eEdition  
**SUBSCRIBE**

# Cancer doctor seeks to withdraw guilty plea in child porn case

By Gabrielle Banks | June 1, 2016 | Updated: June 1, 2016 9:43pm



6



Photo: Jon Shapley, Staff



**IMAGE 8 OF 8**

Former MD Anderson pediatrician Dennis Hughes has asked a federal judge to withdraw his guilty plea.

---

GALVESTON - A former pediatrician at MD Anderson Cancer Center asked a federal judge Wednesday to withdraw his guilty plea to child pornography charges, joining a multistate challenge to an FBI sting using a so-called "dark web" server that led to the arrests of more than 100 people across the U.S.

The challenges - which have been made in at least seven states - could jeopardize the government's ability to investigate cyber-crimes, particularly child pornography sites that often are conducted on anonymous servers, according to federal officials.



The potential unraveling of the government's cases in the sweeping Operation Pacifier sting in Texas and several other states follows a federal court ruling in Massachusetts that the government had no authority to reach into computers outside the area where the search warrants are authorized.

The ruling, which ultimately could be decided by the U.S. Supreme Court, would effectively prevent agents from tracking down people who access child pornography sites or other dark-web enterprises.

"I'm not surprised to hear that defendants are trying to walk back their guilty pleas," said Mark Rumold, a senior attorney at the Electronic Frontier Foundation, a nonprofit focused on civil liberties protections in the digital world.

---

"I think the trend we're seeing - of courts suppressing the evidence stemming from the government's use of malware - is only going to continue."

### ***Guilty plea in March***

Dr. Dennis P.M. Hughes was a tenured professor of pediatrics and a pediatric oncologist at MD Anderson for 11 years before his arrest last summer.

Hughes, 50, of Pearland, pleaded guilty in March to all the charges against him, admitting he collected thousands of images and videos of child pornography on his home and work computers. He remains free on bond.

Hughes filed a motion in April in federal court, however, to withdraw his plea. His lawyer, Neal Davis, asked U.S. District Judge George C. Hanks Jr. on Wednesday to allow the change in the wake of court decisions in Massachusetts and Oklahoma suppressing evidence gathered in the case.

The federal criminal code allows defendants to take back a plea prior to sentencing, and the circumstances in this case are very unique, he said.

"I don't think the floodgates will open," he said.

Assistant U.S. Attorney Sherri Zack, however, argued that permitting Hughes to withdraw his plea "sets a terrible precedent." Zack said Hughes waived his rights and knew what he was doing.

"Mr. Hughes is a doctor. He is not a stupid man by any stretch of the imagination," she said. "There was no mistake."

The judge took the former pediatrician's request under advisement and said he would rule as soon as possible. At least one other defendant in the Houston area has also retreated from a guilty plea.

Federal agents discovered Hughes' hidden pornography stash as a result of a nationwide sting dubbed Operation Pacifier in which they seized control of the server for a dark website called Playpen - where visitors downloaded and shared child pornography.

Federal agents kept the site running at an FBI facility in Virginia for about two weeks while they traced back links to people who visited the site.

Dark websites like Playpen operate on Tor, or The Onion Router, a software that encrypts identifying information for visitors and the hosts.

A U.S. magistrate judge in the Eastern District of Virginia granted the FBI a 30-day warrant to launch hacking software that could help agents bypass the encrypted identities of Playpen visitors and access their IP addresses. The sting led to charges against more than 135 defendants around the country, including seven in the Southern District of Texas, which includes Houston.

### ***Broad searches criticized***

In recent months, federal defendants in Pennsylvania, Ohio and Wisconsin have asked to suppress evidence obtained through the Virginia search warrant on the Playpen server. The judges in all three cases denied these requests.

A district judge in Massachusetts, however, ruled that the Virginia court overstepped its bounds in issuing such a broad warrant, saying the FBI could not extend its search beyond the Eastern District of Virginia. The judge ruled that evidence collected from the defendant's computer could not be used in the case.

A federal magistrate judge in Oklahoma recommended a similar ruling to a district judge. And in Washington state, an Operation Pacifier defendant was granted a request to suppress evidence discovered as a result of the Virginia warrant.

A proposal to revise the federal rules of procedure governing search warrants is now pending before the U.S. Supreme Court. Civil liberties proponents believe the new rules would allow magistrate judges to authorize remote electronic searches of devices anywhere in the world.

The rules are set to go into effect in December unless Congress acts to change the provisions.

A bipartisan group of U.S. senators recently introduced legislation to limit local police and federal investigators' use of broad searches.

Sen. Ron Wyden, D-Ore., who co-authored the "Stop Mass Hacking" bill, said the searches go too far.

"There's no question the rules should keep up with the digital age to ensure law enforcement has the tools needed to go after perpetrators," he said, "but that has to include appropriate protections for law-abiding Americans including those who are victims of hacks."

The Department of Justice welcomes the rule changes, saying they would offer additional guidance to federal judges and magistrates, spokesman Peter Carr said.

The new rules would still require probable cause to believe a crime is being committed and compliance with the Fourth Amendment's protection against unlawful searches and seizures, officials said.

The rules allow agents to ask a single judge - rather than many - to investigate an illegal dark website through malware and go after so-called botnets that remotely seize personal and financial information.

"The various rulings in these cases highlight why the government supports the clarification of the rules of procedure currently pending before the Supreme Court," Carr said, "to ensure that criminals using sophisticated anonymizing technologies to conceal their identities while they engage in crime over the internet are able to be identified and apprehended."

---

---

**Gabrielle Banks**

Reporter, Houston Chronicle

**HEARST** newspapers

© 2013 Hearst Newspapers, LLC.