



Dark web offers anonymity for legal, illegal purposes

April 10, 2016 | Updated: April 10, 2016 11:10pm



The dark web refers to the hidden portion of the Internet where secret and sometimes illegal information can be shared anonymously.

Some dark websites, such as Silk Road, sell illegal narcotics. Some are used to share stolen credit card information. Others, like Playpen and Pedoboard - shut down in recent years by federal agents - are gathering places to share child pornography.

Not all dark websites are illicit, however. Some are used for legal purposes, such as for military business, whistleblowing or for people to speak freely in countries where political speech is controlled.

It's different from the Internet that most people use - known as the clearnet among experts. On the dark web, users' movements are encrypted, making it difficult to trace them.

Here are some key differences between the clearnet and its dark web counterpart:

The clearnet is searchable by law enforcement or anyone else with the skills or a court order to hack into a computer. Those searches allow investigators to identify a person in their home or workplace who ventures onto a public site.

Some clearnet websites offer encryption for things like online bill paying or video-on-demand purchases. But elsewhere a person's identifying information, or IP address, is traceable. Police can subpoena the Internet service provider for details on who signed up for the service.

The dark web offers a hidden route to accessing the same sites that can't be traced back to an IP address. To view the sites, you must download a special browser that re-routes you through an intentionally circuitous path, from one server to another - the



RELATED



Federal agents sweep child pornography site by hacking 'dark web'



7 arrested in child porn sting charged in Houston court

online equivalent of a
blocked phone number.

**Former pediatric doctor pleads guilty to child
porn**

The most common avenue to the dark web is through something called "the onion router," or Tor. Tor websites and Tor website visitors are tagged with an automatically generated code that encrypts communications on both ends. Some Tor sites exchange illicit and illegal information, and some are above-board and legal. The same is true for users. Some have legitimate and legal business purposes that are aided by anonymity.

When the FBI seized the Tor network server used by the Playpen child pornography site in February 2015, agents got a search warrant from a magistrate judge in Virginia authorizing them to use special malware to hack into users' computers. The malware infects the computers and allows agents to bypass the Tor encryption and find the IP addresses of the users on the site. Agents then were able to trace the addresses back to the individuals who had used them.

Gabrielle Banks



HEARST *newspapers*

© 2013 Hearst Newspapers, LLC.