

COMPUTING

Illuminating the Dark Web

It might sound scary, but the ‘dark web’ is not much different from the rest of the internet

By Robert Gehl, The Conversation US on October 31, 2018



Credit: Thomas Trutschel *Getty Images*

*The following essay is reprinted with permission from
The Conversation, an online publication covering the latest research.*

In the wake of recent violent events in the U.S., many people are expressing concern about the tone and content of online communications, including talk of the “dark web.” Despite the sinister-sounding phrase, there is not just one “dark web.” The term is actually fairly technical in origin, and is often used to describe some of the lesser-known corners of the internet. As I discuss in my new book, “Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P,” the online services that make up what has become called the “dark web” have been evolving since the early days of the

commercial internet—but because of their technological differences, are not well understood by the public, policymakers or the media.

As a result, people often think of the dark web as a place where people sell drugs or exchange stolen information—or as some rare section of the internet Google can't crawl. It's both, and neither, and much more.

ADVERTISEMENT

SEEKING ANONYMITY AND PRIVACY

.....

In brief, dark websites are just like any other website, containing whatever information its owners want to provide, and built with standard web technologies, like hosting software, HTML and JavaScript. Dark websites can be viewed by a standard web browser like Firefox or Chrome. The difference is that they can only be accessed through special network-routing software, which is designed to provide anonymity for both visitors to websites and publishers of these sites.

Websites on the dark web don't end in ".com" or ".org" or other more common web address endings; they more often include long strings of letters and numbers, ending in ".onion" or ".i2p." Those are signals that tell software like Freenet, I2P or Tor how to find dark websites while keeping users' and hosts' identities private.

Those programs got their start a couple of decades ago. In 1999, Irish computer scientist Ian Clarke started Freenet as a peer-to-peer system for computers to distribute various types of data in a decentralized manner rather than through the more centralized structure of the mainstream internet. The structure of Freenet separates the identity of the creator of a file from its content, which made it attractive for people who wanted to host anonymous websites.

Not long after Freenet began, the Tor Project and the Invisible Internet Project developed their own distinct methods for anonymously hosting websites.

Today, the more commonly used internet has billions of websites—but the dark web is tiny, with tens of thousands of sites at the most, at least according to the various indexes and search engines that crawl these three networks.

ADVERTISEMENT

A MORE PRIVATE WEB

The most commonly used of the three anonymous systems is Tor – which is so prominent that mainstream websites like Facebook, The New York Times and The Washington Post operate versions of their websites accessible on Tor’s network. Obviously, those sites don’t seek to keep their identities secret, but they have piggybacked on Tor’s anonymizing web technology in order to allow users to connect privately and securely without governments knowing.

In addition, Tor’s system is set up to allow users to anonymously browse not only dark websites, but also regular websites. Using Tor to access the regular internet privately is much more common than using it to browse the dark web.

MORAL ASPECTS OF ‘DARK’ BROWSING

Given the often sensationalized media coverage of the dark web, it’s understandable that people think the term “dark” is a moral judgment. Hitmen for hire, terrorist propaganda, child trafficking and exploitation, guns, drugs and stolen information markets do sound pretty dark.



Sign up for *Scientific American's* newsletters.

[Sign Up](#)

Yet people commit crimes throughout the internet with some regularity—including trying to hire killers on Craigslist and using Venmo to pay for drug purchases. One of the activities often associated with the dark web, terrorist propaganda, is far more prevalent on the regular web.

Defining the dark web only by the bad things that happen there ignores the innovative search engines and privacy-conscious social networking – as well as important blogging by political dissidents.

ADVERTISEMENT

Even complaining that dark web information isn't indexed by search engines misses the crucial reality that search engines never see huge swaths of the regular internet either—such as email traffic, online gaming activity, streaming video services, documents shared within corporations or on data-sharing services like Dropbox, academic and news articles behind paywalls, interactive databases and even posts on social media sites. Ultimately, though, the dark web is indeed searchable as I explain in a chapter of my book.

Thus, as I suggest, a more accurate connotation of “dark” in “dark web” is found in the phrase “going dark”—moving communications out of clear and public channels and into encrypted or more private ones.

MANAGING ANXIETIES

.....

Focusing all this fear and moral judgment on the dark web risks both needlessly scaring people about online safety and erroneously reassuring them about online safety.

For instance, the financial services company Experian sells services that purport to “[monitor the dark web](#)” to alert customers when their personal data has been compromised by hackers and offered for sale online. Yet to sign up for that service, customers have to [give the company all sorts of personal information](#)—including their Social Security number and email address—the very data they’re seeking to protect. And they have to hope that Experian doesn’t get hacked, as [its competitor Equifax was](#), compromising the personal data of [nearly every adult in the U.S.](#)

It’s inaccurate to assume that online crime is based on the dark web—or that the only activity on the dark web is dangerous and illegal. It’s also inaccurate to see the dark web as content beyond the reach of search engines. Acting on these incorrect assumptions would encourage governments and corporations to want to monitor and police online activity—and risk giving public support to privacy-invading efforts.

ADVERTISEMENT

This article was originally published on [The Conversation](#). Read the [original article](#).

ADVERTISEMENT

ABOUT THE AUTHOR(S)