To the Editor June 22, 2020

What is the Dark Web all about?

The World Wide Web, also called the Surface Web or Clear Web (mostly not encrypted or encoded to prevent easy viewing, thus clear), is a part of what you know as the Internet. It is now more than a billion websites, (including mine at www.tcw.org) that a typical search engine used now by more than three billion worldwide users. You access it with a web browser such as Microsoft Internet Explorer, Google Chrome, or better yet Mozilla Firefox.

The Deep Web, (we are talking about Deep not Dark here) is also a part of the Internet and is anything that a standard search engine cannot access outside the enormous one billion. Some estimates are as high as four billion, or so websites existing on servers around the globe. Spiders or also called bots are computer code that crawl the surface web to populate the search engine databases but they cannot reach into the Deep Web.

Deep Web content can be found almost anytime you navigate away from a typical search engine and do a search directly in a website – government databases and libraries contain huge amounts of Deep Web data. Searching the archives of a newspaper is an example of the Deep Web. It can also mean that Internet network router settings have deliberately or accidentally made so that accessing these hosts virtually impossible. Some estimates put this part of the Internet at 400 to 500 times larger than the Surface Web.

For example if you navigate to www.badgerbank.bank/ and login, it will take you to https://secure1.ufsdata.com/PBI_PBI1151/?Token=…

Alternatively, if you navigate to www.ssa.gov and login, it will take you to https://secure.ssa.gov/mySSA/start

These are both secure https, Hypertext Transfer Protocol Secure (HTTPS) sites. This an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over computer network sites in Deep Web.

So that is what the Deep Web consists of, here are some of the things you can find on the Deep web (exclusively talking about the Deep web, excluding the Dark Web) which should further clarify this explanation-

- Password protected pages.
- Attendance records, Medical certificates etc.
- Bank records
- Encrypted Chat Messages (WhatsApp, Facebook Messenger etc.)
- E-mails sent between users
- Purchase-requiring content when not indexed on Search Engines (songs/ videos, courses etc.)

So concisely, the content, which exists on the Internet, but cannot be accessed via Search engines, or requires special permission is Deep Web content.

Some websites also intentionally “de-index” themselves, so that they can only be accessed by people who know the exact URLs, these websites too are a part of the Deep Web, and host thing such as harmless discussions on conspiracy theories, and other such stuff.

As you may have guessed by now, not all un-indexed content is “illegal” or harmful, the Deep Web is not illegal, and it is purely “non-indexed” content.

There is also a parallel Internet, which is accessed by a special browser and home to a freewheeling collection of sites for everything from anonymous activism to illicit activities. Not to mention regular people who do not wish to be surveilled.

The Dark Web (sometime called the DarkNet) is a small portion of the Deep Web that has been intentionally hidden and is inaccessible through standard web browsers. Dark Webs include Tor, or The Onion Router. The Tor network is an anonymous network that can only be accessed with a special web browser, called the Tor browser. The websites limited to the Tor network have a special .onion address extension like darkweba6le5w52w.onion. Because of this, Tor’s Dark Web is also known as onionland. It is an encrypted network built on top of the existing internet. This is the portion of the Internet most widely known for illicit activities because of the anonymity associated with the Tor network. Although the Dark Web has some nebulous uses, most uses are innocuous. For example, people who want to communicate and associate online without fear of being shut down by a government agency. The Dark Web is much smaller than the Deep Web, and it is made up of numerous types of sites like Bitcoin markets, The Hidden Wiki, and porn sites. It is perhaps most notorious for its anonymous marketplaces that often sell illegal products like drugs, or weapons.

Marianas Web, named for the Marianas Trench, which is the deepest part of the world's oceans, being the supposed deepest part of the Deep Web. The URL’s or addresses, of these web sites hosted on the Tor network, are a random string of sixteen meaningless letters and numbers ranging from A to Z and 1 to 7 followed by a dot onion suffix. Tor, The onion router was developed by US Naval intelligence for military purposes and then later became open source software.

These thousands of sites are enormously difficult to shut down because of the anonymity. It is the home of whistleblowers, political activists, as well as criminal activity of illegal drugs, pornography, pirated books, media, weapons, commercial hacking services, computer exploitation software, etc.

It is also the home of creative people, because they have to be creative to be able to survive there, and so innovation takes place as well.

It is also home to security researchers looking for information that can be obtained from monitoring dark web communications, which suggest network intrusions and hackers selling private information captured by computer break-ins.

These sites can have the high quality appearance and graphics of an Amazon, eBay, or other shopping site, but rather than using a credit card, you pay via a crypto currency like Bitcoin. The entire site is encrypted so that domestic and foreign intelligence cannot see what you are looking at or what you buy.

These sellers of course use pseudonyms, but just like the Clear Web, as they too are governed by user reviews and value positive feedback from their customers. There is competition and choice in this world as well, with prices that routinely fall and quality that improves over time, with timely free shipping and generous return policies.

The Tor software provides anonymity by encrypting your email address and routing the traffic through computers around the world designed to do this.

On the Dark Net, I use the Firefox Tor browser and a VPN to protect myself from criminals, capitalist surveillance, and the NSA. A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN benefit from the functionality, security, and management of a private network. A VPN alone will only encrypt the message between the two end points of the VPN tunnel through the public Internet.

So there you have it, the mysteries of the Deep Web and Dark Net revealed.

"Know that every border you cross, every purchase you make, every call you dial, every cell phone tower you pass, friend you keep, article you write, website you visit, email subject line you type, and data packet your router sends, is in the hands of a system whose reach is unlimited but whose safeguards are not. " NSA whistleblower Edward Snowden in his first encrypted email to filmmaker Laura Poitras.

As Roy Zimmerman sings in his song Hello NSA, "we are fighting freedom here at home so we don't have to fight it, over there"