

9

What Goes on in the Dark Web - Case Studies

In the last few chapters, we've discussed *how* to access the Dark Web securely and anonymously by installing and using various security- and privacy-focused operating systems, together with private browsers and VPNs.

In this chapter, let's discuss *what* goes on in the Dark Web, so you can decide *why* you want to go there. We'll discuss how the Dark Web is used, and talk about the stories (true or not) of what goes on in the Dark Web. Some of these examples will be graphic and detailed (not for the faint of heart), but most importantly, they are not of my invention.

I will retell tales that I've heard, read about, or have direct experience with.

Not all of them will be scary, morbid, or gross. Some will be of a positive nature, outlining how people put the Dark Web to use for whistle-blowing, sharing information, marketing, buying and selling, providing medial help, and much more.

We will cover the following topics in this chapter:

- The good and evil sides of the Dark Web
- Onion websites
- Illegal sales on the Dark Web using Bitcoin

The good and evil side of the Dark Web

Most of what we hear in the media is about criminal activities, such as drugs, weapons, and human trafficking, but in reality, there are many other benevolent and beneficial ways to use the Dark Web.

It's important to understand that the Dark Web provides an environment where people can express themselves freely and without censure (for better or worse), gain access to knowledge or content which otherwise would be very expensive to obtain (or even criminal), and find similarly-minded people, subcultures or hobbies (or any other uniting factor).

As with any tool or technology (and yes, I know I'm paraphrasing), the Dark Web isn't inherently evil.

It's populated by people, and it is these people who use the Dark Web for good or evil. Some say that the original intent of the Dark Web was to be an online Utopia, populated by people of every nation, religion and gender, sharing information freely, and working together for the benefit of all.

Sounds like a science fiction story, I know, but it is a worthy dream, nonetheless.

Somewhere along the way, the criminal element inserted itself (or people simply saw how easy it was to perform criminal activities anonymously on the Dark Web), and since shortly after its creation, the Dark Web has had a negative reputation.

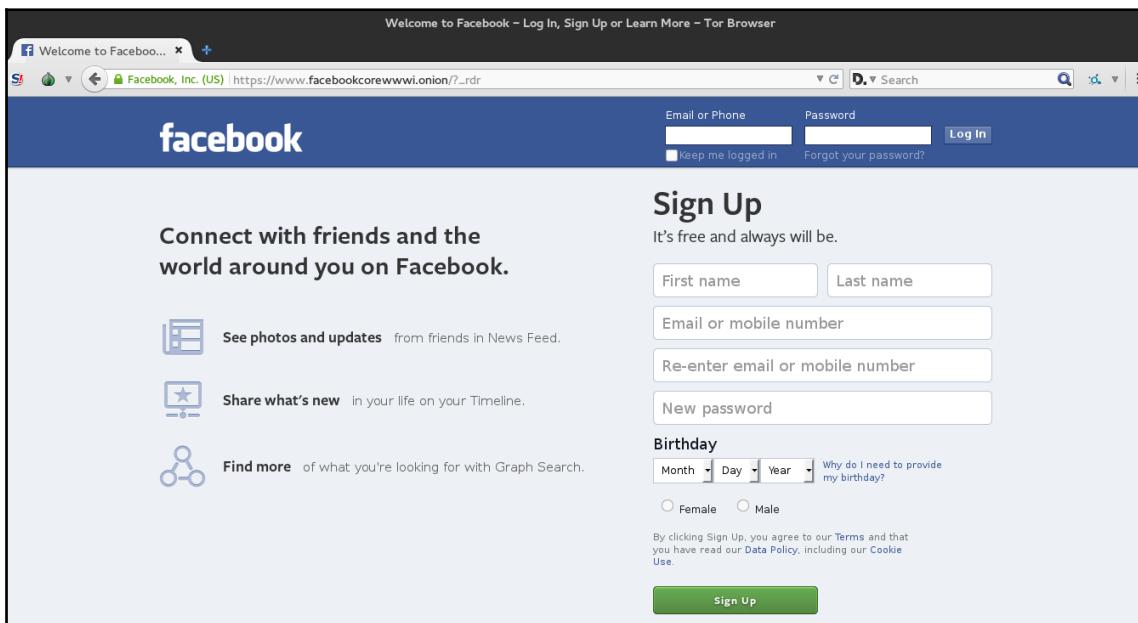
The fact that it's called the Dark Web doesn't necessarily mean that it's evil, but the media and marketers have assigned evil or nefarious qualities to the Dark Web, to enhance sales or consumption of media. What makes the Dark Web so mysterious is the fact that it's not as accessible as **Surface Web** sites. As I explained previously, to access the Dark Web, you need a special browser (Tor, for example), you need to take more precautions, and most importantly, you can't find sites or results from the Dark Web using conventional search engines.

These all enhance the anonymity and privacy that users can take advantage of when browsing the Dark Web.

So let's start. And remember, many of the stories and facts you'll read also exist outside the Dark Web, it's just harder know who you are there, but human nature will always be human nature.

Onion websites

Many companies have started creating websites in the Dark Web, mainly to allow access in countries where there might be prohibitions on using them openly. One example is Facebook, which in October 2014 announced that they had added a Dark Web version in order to prevent access issues that happened when Tor users accessed their accounts through Facebook's regular site. The Dark Web version also allows users from countries that limit access to Facebook to be able to enjoy the social network. The following screenshot displays the Facebook onion site:



Several advertising companies also create sites in the Dark Web, to provide their services to users who want to view ads, but still want to maintain their privacy and security. As you may know, many ads collect information about us, and some are even considered malware. This is one of the reasons that adblockers were developed. For example, Adland, a site boasting the largest collections of Super Bowl commercials in the world, curates and displays ads and commercials from the whole world. They launched a Dark Web site, to protect their readers/surfers.

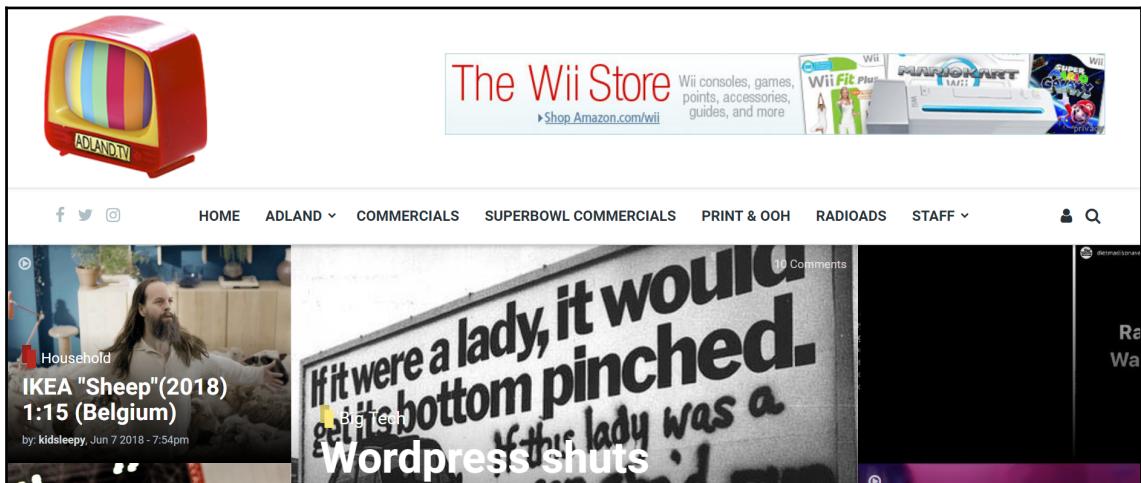
Here is a statement from the founder of Adland:

"Adland's target cares about privacy. We have two different types of readers. There are people who work in advertising, and then there are a lot of technical people like gamers who already have adblock installed."

Additionally, she stated, *The way ad networks (on the Surface Web) are today are basically indistinguishable from malware. There's a lot of third-party calls going on between the publication that you're reading and the [tracker] on the publication.* She views the Dark Web as a mega adblocker, preventing the tracking of data with cookies.

So you could say that hosting an ad site on the Dark Web helps ensure that the ads are legitimate and do not contain malware or cookie-collecting options.

The following picture is of the Adland website:



ProPublica, an American independent, Pulitzer prize winning, nonprofit news site that produces investigative journalism dedicated to exposing incidents and stories that betray the public trust, also launched a Dark Web site, which makes it easier for whistle-blowers and other people who want to share news anonymously to disseminate their information.

The following screenshot is of ProPublica's website:

The screenshot shows the ProPublica homepage with a dark-themed design. At the top, there is a navigation bar with links to "Electionland", "ProPublica Illinois", "Local Reporting Network", and "Data Store". On the right side of the header are social media icons for Facebook, Twitter, and a red "Donate" button. Below the header, the ProPublica logo is prominently displayed. To the right of the logo is a sign-up form for email newsletters with fields for "Email address" and a "Subscribe" button. A large, stylized illustration of a person's head and eye is on the left side of the page. The main article headline is "You Snooze, You Lose: Insurers Make The Old Adage Literally True" under the category "HEALTH INSURANCE HUSTLE". Below the main article are two smaller stories: "Fuel to the Fire" and "Inside Trump's VA". On the right side, there is a "Featured Series" section for "DOCUMENTING HATE" with a thumbnail image showing a large yellow "X" over a dark background.

Everyday users, who began receiving web-search-based targeted ads, started looking for a way to keep their search habits private. Anonymous commerce is something that Facebook, Google, and others view as a significant threat, since one of their best marketing tactics is to monitor users' searches, and track them, followed by targeted ads.

As I indicated previously, dissidents and activists in oppressive regimes use the Dark Web to communicate so they don't get in trouble with their government – sadly there are still governments that limit outside communication through standard channels – or to report what they are experiencing to the outside world.

A report by the Human Rights Watch, a global non-profit, non-governmental human rights organization, called *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* actually discusses this and recommends that human rights workers throughout the world use the Dark Web to communicate securely and privately.

The following screenshot is of the Human Rights website:



In East Asia, Tor is used to ensure anonymity when people reveal information about sweatshops and other labor law problems.

Many situations that you hear about, or see in movies and TV shows, such as fighting the domination of a local town in the eastern US by a large corporation, is done via the Dark Web, by rallying local residents, and planning their actions anonymously and privately.

Human rights activists, working in dangerous areas, use the Dark Web to anonymously report abuse while avoiding prosecution.

Bloggers use Tor for anonymity, and band together to help each other and to promote freedom of speech. An example is Global Voices, an international and multilingual community of volunteering bloggers, journalists, translators, academics, and human rights activists. Their aim is to leverage the power of the internet to build understanding across borders.

They have a newsroom team to report on topics that rarely reach the regular media channels, and they translate the reported stories into numerous languages to break down language barriers.

The following screenshot is of the Global Voices website:

The screenshot shows the Global Voices homepage. At the top, there's a navigation bar with links to various languages: English, Español, Ελληνικά, русский, Malagasy, Français, Português, عربى, ਪੰਜਾਬੀ, Italiano, polski, Esperanto, Nederlands, and македонски. Below the navigation bar is the Global Voices logo. The main content area features a large image of a group of people standing in front of a screen displaying the Google logo in Chinese characters (谷歌). A caption below the image reads: "5 hours ago How will Google plug into China's all-encompassing internet censorship regime? Written by Afef Abrougui · East Asia". To the right of this image is another smaller image showing a group of people holding a protest sign that says "Facebook". Below this image is a section titled "Billions served? Human rights in the Facebook era" with a subtext about tracking hate speech, harassment, and political censorship. There are also links to "Show all Special Coverage »". The footer of the page includes a "Search" bar and social media icons for Facebook, Twitter, and RSS.

They also have a team advocating freedom of speech online. Called Advox, they're part of Global Voices, and according to their website, they *report on threats to online speech, share tactics for defending the work and words of netizens, and support efforts to improve Internet policy and practice worldwide*.

The following screenshot is of the Advox website:

The screenshot shows the Advox website with a red header. The header features the Advox logo (a stylized ampersand and the word "advox") and the text "Global Voices". Below the logo, it says "A project of Global Voices, we are a global anti-censorship network of bloggers and activists dedicated to protecting freedom of expression online." A navigation bar below the header includes links for Censorship, Privacy, Netizen Report, Campaigns & Research, About Us (which is highlighted in yellow), and Archives. To the right of the navigation bar is a search bar and a magnifying glass icon. The main content area has a white background. On the left, there's a sidebar with social media icons for Twitter, Facebook, YouTube, and Google+. The main text area contains two paragraphs: one about Advox's mission and another about their recognition of universal human rights. At the bottom, there's a paragraph about their aim to leverage networks and voices. On the right side, there's a sidebar titled "All Pages" with links to About Advox, Logos, Authors, Attribution Policy, Get Involved, Contact, and Communication safety guidelines. There's also a note indicating the post can be read in French, Italian, and Russian.

About Advox

Advox is a project of [Global Voices](#). We are a global network of bloggers and online activists dedicated to protecting freedom of expression and free access to information online. We report on threats to online speech, share tactics for defending the work and words of netizens, and support efforts to improve Internet policy and practice worldwide.

We recognize that universal human rights to free expression, access to information, and privacy are being challenged by governments, companies, and other powerful actors worldwide. With over 800 contributors in 130 countries, we believe that the Global Voices community is uniquely positioned to do something about this.

We aim to leverage our great strength – our networks, our knowledge, and the voices we seek to amplify – to make our site a central space for anyone eager to learn about

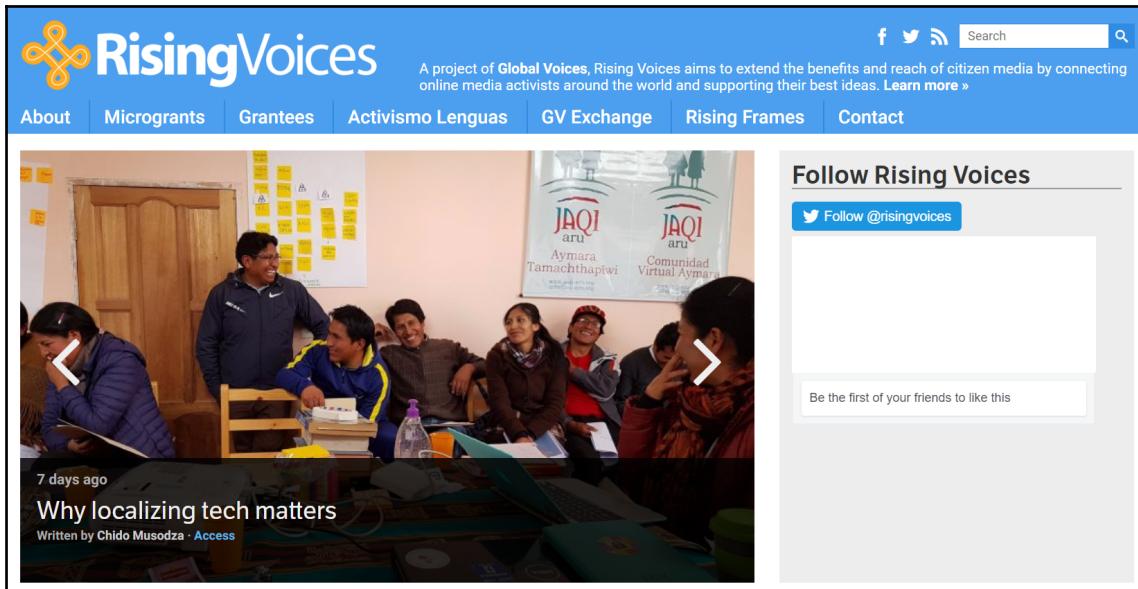
Read this post in [Français](#), [Italiano](#), [русский](#)

All Pages

About Advox
Logos
Authors
Attribution Policy
Get Involved
Contact
Communication safety guidelines

Another team, called Rising Voices, aims to provide training, resources, micro-grant funding, and mentoring to underrepresented communities that want to share their stories using media such as blogs, wikis, media sharing (video/audio/photos), podcasts, and vlogs.

The following screenshot is of the Rising Voices website:



Journalists use the Dark Web to communicate with their sources anonymously, and many news companies (such as The Washington Post, The New York Times, CBC, ProPublica, Dagbladet, and the Associated Press), have lockboxes there, such as SecureDrop, for people to send information and tips to in a secure and anonymous manner. An example of a Dark-Web-based news organization is Reporters without Borders, which is an organization that fights for freedom and protects journalists worldwide.

Lawyers, investigators, and reporters investigating governments use it to avoid being hacked or prosecuted.

The following screenshot is of the SecureDrop website:



Another common use for the Dark Web is to obtain medical advice and medical drugs. Some people are embarrassed to approach a doctor they know and ask questions, and not having to reveal your true identity can help ease that anxiety. Others ask about the possible dangers of combining different drugs, and even just asking about drugs they were prescribed, their effectiveness, side effects, and more. Others attempt to obtain drugs they need and wouldn't have the opportunity to obtain otherwise.

A well-known story revolves around DoctorX, also known as Dr. Fernando Caudevilla, from Madrid, Spain, who provides volunteer medical and drug advice on the Dark Web.

Working as a family physician by day, by night he's answered over 1,000 questions about drugs in forums on Silk Road 1, Silk Road 2, and The Hub.

DoctorX believes drugs should be a question of personal freedom and advocates legalization.

He works for Energy Control, a Spanish organization focused on harm reduction for recreational drug users.

The following screenshot is of the Energy Control website:



Now what about normal people? Many people use the Dark Web to find information or media that would be harder to find, or too expensive to buy on the Surface Web.

Tor and the Dark Web help protect our privacy while we're online. Sadly, many legitimate organizations can have unscrupulous employees, selling our private information. For example, ISPs sell customers' browsing information and history (which includes any search performed, website visited, and possibly usernames and passwords) to marketing companies, after supposedly anonymizing the data, something that is not always correct. Sadly, this information can also be obtained from the search engines we use, the social networks we're members of, and the websites we visit.

Many of you may have heard of GDPR, the European General Data Protection Regulation, a regulation focused on data protection and privacy for all individuals within the **European Union (EU)** and the **European Economic Area (EEA)**.

GDPR was created to give individuals control over their personal data and to provide regulations to businesses regarding how to treat the personal data of their employees, customers, or business partners. GDPR applies to an enterprise established in the EEA or – regardless of its location and citizenship – that is processing the personal information of individuals or businesses inside the EEA.

GDPR requires these businesses to put in place *appropriate measures, both technical and organizational* to implement the data protection principles it provides, and to use the highest-possible privacy settings by default. This ensures the data is not publicly available without explicit, informed consent from the individuals, and that the data cannot be used to identify them without additional information, which is stored separately.

These measures already exist on the Dark Web, by default, especially if you use Tor or another darknet, which is why many people use them – to prevent the betrayal of their private data.

The vast majority of Dark Web users are privacy- and anonymity-focused people, so unless you provide information yourself, decline to use the standard precautionary measures we've discussed (which is comparable to explicit, informed consent), or if you're maliciously attempting to collect information about people, you'll actually be implementing GDPR, de facto – using appropriate measures to protect personal data.

The following screenshot is of the EU GDPR website:



Additional uses of Tor (both on the Dark Web and the Surface Web) include protecting children, by obfuscating their IP address and preventing anyone from detecting the child's location. Naturally, Dark Web access should be regulated by parents, to prevent their children from accidentally (or intentionally) accessing the less-savory and illegal sites that exist there, but using Tor on the Surface Web is good enough.

Since one of the original goals of the Dark Web was information sharing, without censorship, there's a lot of it there. Many people perform research on any number of subjects, which might be sensitive and thus marked for monitoring by the NSA or any other governmental agency around the globe, or simply because they don't want to expose the information they're researching to their friends and family.

Many public figures have private blogs, forums, or websites on the Dark Web, allowing them to communicate their ideas and beliefs without compromising their public image. This is true for celebrities, political figures, and basically any person who is in the public eye.

Now, what about information sharing? There are many communities that share training and guides, regarding any number of subjects, from criminal activities such as hacking, counterfeiting documentation, and manufacturing drugs or other illegal substances, to deep-sea fishing and poetry discussions.

WikiLeaks is a site that is infamous for its political and corporate leaks, whose information is gleaned mainly via the Dark Web, with them posting that information on their Surface Web site.

The following screenshot is of the WikiLeaks website:

The screenshot shows the WikiLeaks homepage. At the top, there is a navigation bar with links for 'Leaks', 'News', 'About', 'Partners', 'Shop', 'Donate', and 'Submit'. Below the navigation bar, there is a secondary menu with links for 'Intelligence', 'Global Economy', 'International Politics', 'Corporations', 'Government', and 'War & Military'. The main content area is titled 'Featured' and contains three news items:

- Amazon Atlas**: An image of a map showing various locations marked with blue dots across a geographic area.
- Dealmaker: Al Yousef**: An illustration of a man in a yellow t-shirt with 'UAE' on it, standing behind a green tank. The background shows flags of the UAE and Yemen.
- ICE Patrol**: An image of the Earth with a magnifying glass icon over it. Below the image, text reads: "ICE Patrol is a searchable archive of U.S. Immigration and Customs Enforcement (ICE) employees with LinkedIn profiles."

There are also many sites that are book clubs or that offer books, such as Bibliomaniac. It's said that you can find any book in the world on their website, but be careful and don't do anything illegal, such as downloading copyrighted content.

Just like on the Surface Web, music is accessible on the Dark Web, but much more so. Almost all of it is free.

Some Dark Web sites just display pictures or slideshows, such as Tor Kittenz, while others display reprehensible content, such as live tortures, murders, and kidnappings, and even worse things. I've heard of some that display images of injuries and accidents (similar to Ogrish or Gorish on the Surface Web, but worse, if that's possible). Sites displaying dead bodies, in general, are not so rare. And others allow you to get answers on truly anything. Hidden Answers, for example, is the Dark Web version of Reddit, where you can ask or share anything you want.

The following screenshot is of the Hidden Answers website:

The screenshot shows the homepage of the Hidden Answers website. At the top, there is a navigation bar with links for Questions, Unanswered, Tags, Users, Ask a Question, Badges, Rules, and Contact. Below the navigation bar, a banner reads "Welcome to Hidden Answers. Make sure you're on [answers.tdhtbeek.onion](#)" and provides links for Español, Português, and Русский, along with the I2P address [hiddenanswers.i2p](#). The main content area is titled "Recent questions and answers". It displays four recent posts:

- Where can I get a phone number which I can use on Gumtree or Craigslist and it wont get me tracked?** (1 answer, 0 upvotes, 0 downvotes) - Answered 8 minutes ago in Technology by 0x2622 Novice (1,420 points). Tags: trading, analysis, money, community.
- Algorithmic Trading** (2 answers, 0 upvotes, 0 downvotes) - Answered 19 minutes ago in Markets by 0x2622 Novice (1,420 points). Tags: trading, analysis, money, community.
- Feeling responsible for everything** (4 answers, 0 upvotes, 0 downvotes) - Answered 22 minutes ago in Other by 0x2622 Novice (1,420 points). Tags: feeling, responsible, for, everything.
- AMD vs Intel for virtualization** (1 answer, 0 upvotes, 0 downvotes) - Answered 31 minutes ago in Technology by 0x2622 Novice (1,420 points). Tags: cpu, amd, intel, virtualization, linux.

To the right of the posts, there is a sidebar with two sections:

- Please read: Important information about new HA administration and future site direction**: A note from the site administrator about changes to the site's administration and future direction.
- Rules have also been updated; please read them**: A note from the site administrator about updated rules.

Below these notes, there is a message from the administrator about the site's future direction and民主化.