The Dark Web  
Opposition Brief by Steven Errico



Some Affirmatives for this resolution use fear to their advantage by referencing some of the scary things that happen when privacy gets out of hand. A lesser-known but powerful application of this is the dark web argument.

According to Investopedia, “The dark web refers to encrypted online content that is not indexed on conventional search engines. The dark web is part of deep web, a wider collection of content that doesn't appear through regular internet browsing. A specific browser like Tor is required to access dark web sites. The dark web holds anonymous message boards, online markets for drugs, exchanges for stolen financial and private data, and much more. Transactions in this hidden economy are often made in [bitcoins](https://www.investopedia.com/terms/b/bitcoin.asp) and physical goods are shipped in a way to protect both the buyer and seller from being tracked by law enforcement.” (<https://www.investopedia.com/terms/d/dark-web.asp>)

I don’t have access to a published case that uses this application, but the argument goes something like this: *Privacy is good, but it has to be kept in check. The dark web is an example of what happens when privacy is valued over truth-seeking. This is where criminals go when they want privacy. Since the online activity on the dark web is difficult to track and uncover, criminals can get away with horrible crimes–such as selling illegal drugs and distributing child pornography–without much chance of being caught. Since truth-seeking is not upheld, problems occur, and the same will be true outside of the internet and on the streets if privacy is valued above.*

The dark web argument is one of many ways Affirmatives try and show the judges what privacy looks like when it has gone too far. Think of it as the Affirmative equivalent to the 1984/Orwellian Society argument that Negatives will sometimes use. The problem with these types of examples, however, is that they are rarely simple enough to actually prove their point without creating some issues. It is rarely that easy. As Prince Charming says in *Shrek the Third*, “There are two sides to every story, and our side has not been told!” The goal of this brief is to demonstrate how the dark web argument really does not fit the narrative of privacy gone wrong.

What you will probably end up doing is creating something of a common ground between yourself and the Affirmative: We can all agree that the dark web has enabled criminals to do things that we most definitely should not approve of. The point is, don’t let the Affirmative back you into a corner and force you to support everything about the dark web when you really don’t have to. This brief will give you plenty of evidence that you can use in your rounds to refute the idea that the dark web is just an example of privacy gone wrong.

The same methodology used in this brief can be used to refute basically any other similar argument. If your opponent uses extreme examples, show why they don’t prove anything.

The Dark Web

Criminals on the Dark Web Harm the Privacy of Others

Torres, Elise. “5 Worst Criminals Caught On The Dark Web.” TruthFinder, Crimewire, 9 May 2018, [www.truthfinder.com/infomania/dark-web/5-worst-dark-web-criminals/](http://www.truthfinder.com/infomania/dark-web/5-worst-dark-web-criminals/).

Here are five of the worst offenders caught on the Dark Web. 1. Peter Scully - The infamous Australian pedophile potentially faces the death penalty in the Philippines. He faces a litany of charges, but the world knows him for the sickening film known as “The Destruction of Daisy.” The details of his crimes are simply too grotesque for public discussion. Scully has been charged with masterminding a worldwide criminal network, as well as producing and selling videos that show child sex abuse and torture. He faces a total of 75 charges. Unless the death penalty is reintroduced, Scully may face the maximum sentence of life imprisonment and a total of 100 years in jail. 2. Marcel Hesse - Marcel Hesse, 19, stabbed his neighbor's 9-year-old son more than 50 times. Shortly after, he stabbed his 22-year-old friend over 60 times and set his apartment on fire. The German teen bragged about the child’s murder online and uploaded the harrowing footage and pictures to the Dark Web. He voluntarily surrendered to police after a nationwide manhunt. Earlier this year, he was sentenced to life in prison, which will be served in a psychiatric ward. 3. Ross Ulbricht - Ulbricht had a bright future: he was a graduate of Penn State with a master’s degree in material science. He wanted to become an entrepreneur — a desire that eventually pushed him to create a drug dealing empire on the Dark Web. Known as the Silk Road, the infamous drug trafficking enterprise earned Ulbricht a fortune of $28.5 million. However, careful use of TOR wasn’t enough to keep him off law enforcement’s radar. He was picked up in San Francisco and charged with money laundering, computer hacking, conspiracy to traffic narcotics, and conspiracy to traffic fraudulent identity documents. He is now serving a life sentence for his efforts, which was upheld in 2017. 4. Shannon Grant McCoole - In 2014, Australian police infiltrated a Dark Web gang that eventually led to care worker McCoole. As well as abusing at least seven children in his care while employed for South Australia’s Department for Child Protection, McCoole was the head administrator of a global child pornography website. In 2015, he was sentenced to 35 years in jail. He recently requested a reduction in his sentence after cooperating with authorities to prosecute a European user of the website. Prosecutor Ian Press argued that McCoole has not shown any sign of remorse for his actions and is only willing to cooperate ‘on his terms.’ 5. Hieu Minh Ngo - Compared to some on this list, Ngo really isn't the worst. In 2015, he was charged with hacking into United States businesses’ computers and selling personal information to cybercriminals — but the sheer scale of his crimes earns him a spot on this list. He gained access to more than 200 million identities and had them all for sale. He made $1.9 million from his illicit activities. He posed as a private investigator to buy details that he then sold on the open market. Ngo could have gotten away with it, but he made a rookie mistake when an undercover Secret Service agent lured him to Guam for a business deal. In 2013, he touched down on US soil, and he was promptly arrested. Two years later, he was sentenced to 13 years in a federal prison.

Protects One’s Privacy at the Expense of Another’s Privacy

Smith, Ed. “Deep Web Search Facts You Need To Know.” TruthFinder, Crimewire, 5 July 2018, [www.truthfinder.com/infomania/dark-web/deep-web-search/](http://www.truthfinder.com/infomania/dark-web/deep-web-search/).

Here are the types of illegal operations you could find on the TOR network: Sale of unlicensed firearms Child pornography Sale of malware, pirated software, and hacking guides Sale of illegal drugs Identity hacks and sale of stolen credit card information and user accounts Sale of forged documents and currency Hiring hit men Gambling Money laundering Insider trading

Users are at Risk

“The Darknet.” INTERPOL, [www.interpol.int/Crime-areas/Cybercrime/The-threats/The-Darknet](http://www.interpol.int/Crime-areas/Cybercrime/The-threats/The-Darknet).

The increasing use of technology and the Internet in all aspects of daily life puts everyday citizens at risk of becoming targets of cybercriminals. As society comes to rely more and more on the Internet, the dangers posed by different types of cybercrime have become very real threats. These threats come in a variety of forms and target different features of the Internet, technological devices and their users.

Malware and Exploitation

“Crime on the Dark Web: Law Enforcement Coordination Is the Only Cure.” Europol, 1 June 2018, [www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure](http://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure).

In recent years several successful coordinated investigations were able to take down some of the largest dark web markets, undermining the assets exploited by criminals. In particular, in summer 2017 joint operations led by the US FBI and the Dutch National Police, with the support of Europol and other law enforcement partners, shut down Alphabay and Hansa, two of the largest marketplaces responsible for the trading of over 350 000 illicit goods like drugs, firearms and cybercrime tools, such as malware.

Identity Theft and Personal Information

LaMagna, Maria. “The Sad Truth about How Much Your Facebook Data Is Worth on the Dark Web.” Market Watch, 6 June 2018, [www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20](http://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20).

People buy other risky or illegal substances on the dark web, including drugs, pirated content like movies or music and materials that help with scams, including credit-card “skimmers.” Facebook logins can be sold for $5.20 each because they allow criminals to have access to personal data that could potentially let them hack into more of an individual’s accounts. The credentials to a PayPal account with a relatively high balance can be sold on the dark web for $247 on average, the report found. One’s entire online identity, including personal identification numbers and hacked financial accounts, can be sold for only about $1,200 on the dark web, Fractl found.

Whistleblowers

Smith, Ed. “Deep Web Search Facts You Need To Know.” TruthFinder, Crimewire, 5 July 2018, [www.truthfinder.com/infomania/dark-web/deep-web-search/](http://www.truthfinder.com/infomania/dark-web/deep-web-search/).

WikiLeaks is a notorious Dark Web site that allows whistleblowers to anonymously upload classified information to the press.

It's Not Very Private Anyway

“Crime on the Dark Web: Law Enforcement Coordination Is the Only Cure.” Europol, 1 June 2018, [www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure](http://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure)

Owing to the success of these operations, the volume of transactions has decreased and some traders have left the dark web platform due to anxiety, uncertainty and the risks regarding the level of anonymity. After the takedown operations, many vendors, who had their shop closed twice in short succession, were not inclined to open them again, while the distrust between vendors and buyers has increased.

The Government Can Infiltrate

Mills, Chris. “Feds Take down Dozens of 'Dark Web' Weapons and Drug Vendors.” BGR, 28 June 2018, <https://bgr.com/2018/06/27/dark-web-drugs-weapons-sites-fbi-investigation/>

The ‘dark web’ — a series of websites accessible through the anonymous Tor browser, which tends to lend a thin veil of anonymity to users — shot to prominence as a place to buy almost anything thanks to a 2011 *Gawker*profile of The Silk Road, the internet’s first big marketplace for almost anything. Law enforcement agencies were horrified of the idea that an Amazon for crime could operate semi-openly, making weapons, drugs, and hacking tools available to anyone with a fistful of cryptocurrency, so despite the fact that dark web sales make up a fraction of the global drug and weapons trade, police organizations worldwide have been cracking down with a vengance. The Department of Justice announced Tuesday that it had arrested 35 individuals charged with selling “illicit goods,” and seized a reported $23.6 million in weapons, drugs, and cryptocurrency. The arrests were the culmination of a “year-long, coordinated national operation that used the first nationwide undercover action to target vendors of illicit goods on the Darknet.” In the press release, the DoJ said that an agent from Homeland Security Investigations posed as a money launderer who would buy cryptocurrency — the way money usually changes hands in Dark Net transactions — for US cash. Agents were then able to investigate the recipients of the cash, leading to the observation of 65 targets and the arrest of 35 alleged Dark Net vendors. Undercover agents posing as criminals is the feds’ favorite way to tackle online illegal sales, since Tor grants anonymity to criminals and cops alike. In the past, investigators have posed as the administrators of numerous Dark Net websites to gather information, although this appears to the be one of the first operations targeting specific vendors, rather than the people running the sites themselves. “The Darknet is ever-changing and increasingly more intricate, making locating and targeting those selling illicit items on this platform more complicated.  But in this case, HSI special agents were able to walk amongst those in the cyber underworld to find those vendors who sell highly addictive drugs for a profit,” said HSI Acting Executive Associate Director Benner.  “The veil has been lifted. HSI has infiltrated the Darknet, and together with its law enforcement partners nationwide, it has proven, once again, that every criminal is within arm’s reach of the law.”

It’s Non-Unique from the Regular Internet

Gehl, Robert. “Illuminating the Dark Web.” Scientific American, Springer Nature, 31 Oct. 2018, [www.scientificamerican.com/article/illuminating-the-dark-web/](http://www.scientificamerican.com/article/illuminating-the-dark-web/).

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. 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.

It Has its Noble Uses

Choudhury, Saheli Roy, and Arjun Kharpal. “The 'Deep Web' May Be 500 Times Bigger than the Normal Web. Its Uses Go Well beyond Buying Drugs.” CNBC, 7 Sept. 2018, [www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html](http://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html).

The so-called dark web, a portion of the hidden internet, is usually associated with a host of illegal activities including the buying and selling of drugs, firearms, stolen financial data and other types of valuable information. The selling point? Total anonymity. That may sound nefarious, but some experts argue that the dark web is also useful in circumventing internet censorship.

Patterson, Dan. “Dark Web: A Cheat Sheet for Business Professionals.” TechRepublic, 26 Oct. 2018, [www.techrepublic.com/article/dark-web-the-smart-persons-guide/](http://www.techrepublic.com/article/dark-web-the-smart-persons-guide/).

But the Dark Web is not all bad news. ProPublica, a well-respected investigative news organization, has a Dark Web site to help the company securely communicate with sources. The United Nations law enforcement department, the Office on Drugs and Crime, monitors the Dark Web and shares data with the public and global police organizations. Even Facebook, the world's largest social network, has a Dark Web site relied on by over one million users per month.

The Good Guys Use it Too

Smith, Ed. “Deep Web Search Facts You Need To Know.” TruthFinder, Crimewire, 5 July 2018, [www.truthfinder.com/infomania/dark-web/deep-web-search/](http://www.truthfinder.com/infomania/dark-web/deep-web-search/).

Because the TOR network allows users to browse anonymously, it's used by secret service agents, law enforcement, activists, researchers, whistleblowers, and users who are banned from Internet access.

We Can Catch Terrorists on It

McCormick, Ty. “The Darknet: A Short History.” Foreign Policy, 9 Dec. 2013, <https://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/>.

August 4, 2013 - The U.S. government intercepts secret communications between al Qaeda chief Ayman al-Zawahiri and Nasir al-Wuhayshi, the head of the Yemeni-based al Qaeda in the Arabian Peninsula. The online confab leads to the shuttering of U.S. embassies in 21 countries across the Muslim world. According to researchers at the Institute for National Security Studies in Israel, the high-level al Qaeda talks "apparently took place in a part of the internet sometimes called deepnet, blacknet, or darknet."