Spring 2021

An Ethical Analysis of Public Policy and the Dark Web

Emily Tritle

Recommended Citation
Tritle, Emily, "An Ethical Analysis of Public Policy and the Dark Web" (2021). *Creative Components*. 816.
https://lib.dr.iastate.edu/creativecomponents/816

An Ethical Analysis of Public Policy and the Dark Web

By

Emily J. Tritle

A Creative Component submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE

Major: Cyber Security

Program of Study Committee:
Dr. Alex Tuckness, Major Professor

Iowa State University
Ames, Iowa
2021

Table of Contents

List of Figures……………………………………………………………………..………3

Introduction and Purpose………………………………………………………………….4

Background Information…………………………………………………………………..6

Negatives of Anonymous Activity on the Dark Web……………………………………10

Positives of Anonymous Activity on the Dark Web……………………………………..13

The Utilitarian Approach………………………………………………………………...16

The Libertarian Approach………………………………………………………………..23

The Kantian Approach…………………………………………………………………...26

An Ethical Way Forward………………………………………………………………...32

Conclusion……………………………………………………………………………….37

Bibliography……………………………………………………………………………..40

List of Figures

Figure 1 Three Hop Circuit[1]…………………………..……………………………………..9

Figure 2 Directly Connecting Users[2]…………………………………………………………15

[1] Owen and Savage, “The Tor Dark Net,” 1

[2] The Tor Project Website, https://metrics.torproject.org/userstats-relay-country.html.

Introduction and Purpose

"The dark net is the next side of the problem, where pedophiles and perverts are sharing images, not using the normal parts of the internet that we all use."

- David Cameron, Former Prime Minister[3]

"The problem is, unlike a real-world town or city, most people either can't or don't want to visit the dark net so their perception is driven by one-sided reporting. We imagine the worst and fail to see the best."

- Andrew Murray, Journalist[4]

Since its inception, the dark web, sometimes known as darknet, has been a topic of contention among citizens and policymakers alike. As suggested by the above quote from the former Prime Minister of Great Britain, David Cameron, it has often found itself to be the subject of critique by law-abiding citizens who believe that criminals and hackers spend their time lurking there without the threat of surveillance or punishment. These rumors, though perhaps too generalized, are not without merit. However, it is important to understand that there is more to the dark web than simply a method to cover up illicit internet activities or to acquire illegal substances or materials that might be otherwise unavailable for purchase.

There are other, more positive aspects of the dark web that are less frequently mentioned. The anonymous nature of the system allows for journalists and freedom fighters in countries that have heavy censorship laws and internet monitoring to reach out to supporters and sympathizers around the world without fear of being persecuted for their actions. In addition, in our current

[3] BBC, "GCHQ to help tackle 'dark net' child abuse images."
[4] Murray, "The dark web is not just for pedophiles, drug dealers and terrorists."

age of data collection, buying, and selling, more people are realizing that any privacy they thought they had while browsing the surface web is purely an illusion. This has been driving larger numbers of law-abiding citizens to use browsers like Tor that will mask their identity and protect their personal information while they surf the internet.

With the rising traffic on the dark web, greater awareness of what happens there, and big news stories revolving around the tracking and arrest of black-market dealers, we are being faced with a choice now more than ever. Despite its positive uses, the general perception of the dark web remains murky and unfavorable. The opinion of the general population in the United States is that we would be better off shutting the dark web down.[5] The purpose of this paper is to serve as a guide to policymakers as this pressure is continuously mounting. Though it is generally agreed by experts that the dark web will never completely go away regardless of our efforts,[6] some worry that the technology to unmask the anonymity of the dark web is evolving faster than we realize. If or when this technology does materialize, the question we must address is whether or not it would be ethical to dismantle the dark web as we know it.

In order to examine the ethical implications behind this question, I will first present the technical material necessary to understand how the dark web works, why it was created, and how it is used. Contrary to popular belief, there are many benefits that the dark web provides for users around the world. With this in mind, I will discuss both the pros and cons that are associated with its existence. Once that information is established, I will apply three political theories to our question and identify how scholars in each school of thought would answer. First, I will examine utilitarianism. Next, I will present the case from the perspective of libertarians. Lastly, I will look at the argument from a Kantian perspective. These three schools of thought

[5] Greenberg, "Dark Web's Bad Rep."

[6] SecureTeam, “What is the Dark Web & How Does it Work?”

all hold radically different ideas on what is important and how to determine if an action or policy is ethical. My contention is that all three paradigms will, ultimately, come to the same conclusion: it would be unethical to dismantle or regulate the dark web for any policy purposes.

With the mounting pressure on policymakers to institute changes to dark web accessibility, the issue of regulating or dismantling the dark web must be discussed. While many experts have weighed in on the benefits and drawbacks to the dark web, there have been no analyses that offer any sort of input into how policymakers can balance these. Freedom of speech is an important freedom, but upholding the law and protecting victims from cybercrimes is important as well. This paper offers guidance for policymakers wrestling with how to best balance these divergent interests and protect their constituents from infringements on freedom and wellbeing.

Background Information

As indicated in the introduction, rumors and misinformation about the dark web have abounded since its inception. Some say it is a place where only criminals go in search of weapons, drugs, or other materials that can only be found on the black market. Others say that the dark web is frightening simply because of its sheer scale. After all, some experts have estimated the portion of the web that is inaccessible via normal search engines to be up to 550 times larger than the surface web[7]– and growing every minute. However, there are relatively few users of the dark web in comparison with the surface web, so it is important to disentangle truth from myth.

[7] Bergman, "Deep Web: Surfacing Hidden Value."

To begin, it is essential to define exactly what the dark web is. Though the term is sometimes used synonymously with the deep web, the two entities are actually different. The deep web refers to portions of the internet that are not accessible through normal search engines like Google or Bing. In fact, it is noted that, "Google indexes no more than 16 percent of the surface web and misses all of the deep web. Any given search turns up just 0.03 percent of the information that exists online."[8] With such a vast scope, it is no surprise that its existence feels threatening. The deep web includes sites on the dark web, but it mostly encompasses private web pages such as personal email accounts or null pages that are required to redirect visitors to certain websites. This accounts for the enormous scale of the deep web. So, while the dark web is encompassed in the deep web, the deep web is, in itself, not a security concern.

In order to access sites on the dark web, specialized browsers that use particular routing protocols are required. The first private routing browser, known as Freenet, came into existence in March of 2000.[9] Though it did not operate quite like the dark web browsers do now, it was a prototype in anonymous routing. Freenet is still around, but it was not until Tor was created that the dark web started to gain traction. Tor (an acronym standing for The Onion Router) was designed by the United States Naval Research Laboratory for government purposes in 2002. It was quickly released to the public for use in 2004, and the original creators founded the Tor Project in 2006 in hopes of attracting more users and gaining awareness.[10] The idea was that the more traffic routed through this new browser, the harder it would be for anyone to track exactly what the government was doing on the network. Since the military wanted to be able to conduct its business privately, the influx of public users helped mask their activities.

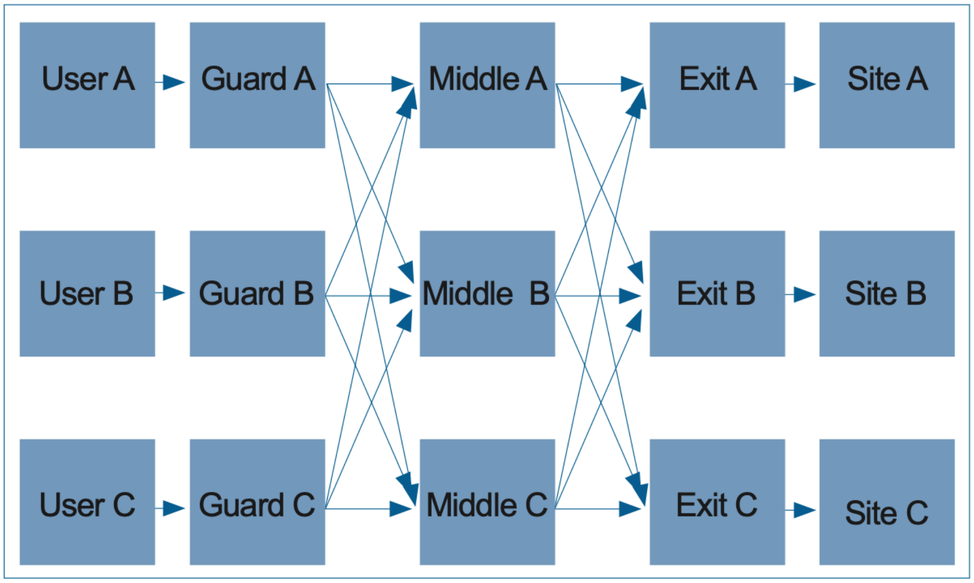
[8] Weimann, "Terrorism on the Dark Web," 196.
[9] Nancy, "The Dark Web: A History Lesson."
[10] Ibid.

Since then, other browsers have been created with similar features to preserve anonymity and reach websites that are not otherwise available on the surface web. The Free Internet Project (I2P) is another popular browser that can be used to access the dark web and operates all domains that end in .i2p. Though I2P has been a successful browser for accessing the dark web, Tor remains the most popular choice. Its early role in developing a secretive routing protocol has put Tor in the perfect position to maintain open access to individuals all over the world and monitor governments' attempts to block its use.

As mentioned earlier, the dark web is special because of its routing protocols. In order to cloak the identity of the user, the Tor browser operates by utilizing thousands of volunteer computers to act as relays. Traffic from a single user, then, will hop through a relay before arriving at the desired site. From an observer's standpoint, the traffic originated at the relay, so it is very challenging to identify the true source. Therefore, while it would be possible to monitor how much traffic a given site was receiving, it would not be easy to determine the identity of the visitors.

However, with the analysis of traffic patterns, the source could eventually be detected if the observer were dedicated and clever enough. Because of this, internet traffic is actually routed through three relays, known as the "three-hop circuit." In this system, there is an entry, guard, and exit relay that route the user to the desired site. This creates an extremely difficult situation for any observer that wants to analyze traffic patterns to uncover the identity of the user. In fact, the only way that it would be feasibly possible to track a user is if the observer is in a position to monitor all three of the random relays that are selected, and this is considered impossible.[11] Coupled with a virtual private network (VPN) for extra security, it is now completely infeasible to track any given user.

Figure 1



An illustration of the three-hop circuit. Source: Owen and Savage, "The Tor Dark Net," 1.

Though the dark web is open for anyone to use, it is not recommended for those that have not taken the proper precautions to protect themselves and their device. It is generally suggested that web cameras should be disconnected and special firewalls enabled to ensure that an unsuspecting device cannot be easily overtaken by a botnet or hacker. The dark web was not designed to be user-friendly or easy to navigate. Unlike the search engines that exist on the surface web, the dark web can only be navigated by existing knowledge of the website you are trying to reach or by using a system of indexes that lists active domains.[12] These indexes are not

[11] Owen & Savage, "The Tor Dark Net," 1.
[12] Weimann, "Terrorism on the Dark Web," 196.

simple to traverse, and it can be easy to stumble across a website that can strip information from your computer or infect it with a virus. In general, it is best to not attempt to navigate the websites on the dark web without the knowledge and expertise on how to do it safely.

With this background information in place and proper warnings given, it may seem pretty clear why there are so many people who advocate against the dark web's existence. However, it is important to have a balanced view when weighing the positive and negative attributes of the dark web. In the following section, I will explain the arguments given by those who favor restrictions on the dark web. Then, I will present arguments for why the dark web is a beneficial addition to the internet. As we shall see, it is not as black and white as many people have been led to believe.

Negatives of Anonymous Activity on the Dark Web

Anonymity has a way of encouraging bad behavior. When a person is unafraid of being held accountable for his actions, it tends to warp his sense of responsibility to do the right thing. The famous story of the Ring of Gyges that was presented in Plato's *Republic* comes to mind when thinking of this phenomenon. In this story, a lowly shepherd obtains a magical ring that allows him to become invisible while wearing it. He immediately goes to work overthrowing the king and stealing whatever his heart desires, since he can do so without anyone drawing a connection between him and his actions. It is argued that even a just man would eventually become corrupted by this immense power. Glaucon, the character that tells this story to convince Socrates that justice is not valuable in itself, concludes, "This we may truly affirm to be a great proof that a man is just, not willingly or because he thinks that justice is any good to him individually, but of necessity, for wherever anyone thinks that he can safely be unjust, there he is unjust."[13]

The Dark Web is a more modern take on the Ring of Gyges. It can, essentially, make the user invisible and disconnect him as a person from his actions. This power has led to some very dangerous and destructive behavior. The connotation of criminals and the dark web forming a symbiotic relationship with each other is not baseless. Famous black markets, such as the Silk Road, have long provided customers with items that would otherwise be unattainable. Or, at least, unattainable without significant risk involved. However, with the ability to mask one's identity, it is easy to buy drugs, weapons, cracked passwords, fake passports, or even hire a computer hacker for whatever nefarious plot one has in mind.

Another serious drawback that this anonymity breeds is the side of the dark web devoted to human trafficking and child pornography. In fact, researcher Gareth Owens spent six months indexing traffic patterns on the dark web and found that sites that hosted this type of material were the most sought after of all the sites on the dark web.[14] Websites like Playpen, which are devoted to this kind of obscene material, reportedly received 11,000 unique visits per week before it was taken down by the Federal Bureau of Investigation (FBI).[15] This is a very serious problem and, despite progress in investigation strategies, it remains very difficult to handle effectively because of the secret routing and inability to identify those that are visiting the sites and those that are uploading content. Rumors around the existence of something called a "red room"– where visitors can watch live feeds of people being tortured– have also circulated widely, though there is little evidence that such sites actually exist even on the dark web.[16]

[13] Plato, "The Republic," 360c.
[14] Weimann, "Terrorism on the Dark Web," 196.
[15] Jardine, "Privacy, censorship, data breaches, and Internet freedom," 2825.
[16] Nancy, "The Dark Web: A History Lesson."

Much of the dark web is composed of sites designed specifically for botnet operations, which presents another nuissance to society. Though these operations are not quite as detrimental as the topics previously discussed, they are still an unfavorable aspect of the dark web. These botnets can be used to scalp commodities off of the surface web for resale at much higher costs. Recently, we saw this happen with the release of the PlayStation 5, though it very frequently occurs with concert tickets and limited-edition items. Botnets can also be used more nefariously with coordinated Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks designed to bring down websites or, on a larger scale, networks as a whole. Though we have ways of mitigating DOS attacks, DDOS attacks remain very challenging to defend against and can cause an enormous amount of trouble for the victims.[17]

Lastly, the dark web is dangerous to navigate for those that are inexperienced. There have been reports of new users finding out that their webcams were hacked in a way that allowed the attacker to activate the device at will.[18] This allows for discrete spying on the victim whenever the desire arises. Some users that stumble across certain websites will find their devices infected with malware or recruited to join a botnet without the choice or knowledge that their device has been enslaved.[19]

Clearly, there are some significant disadvantages to the dark web. Ranging from pesky to downright abhorrent, these stories and issues are often what are talked about when the dark web is brought up in conversation or on the news. While it is right and appropriate to be aware of and discuss these drawbacks, there is another side of the story that is often neglected. Next, I will

[17] Jacobson, "Introduction to Network Security," 71-72.
[18] Tamburro, "You are Being Watched."
[19] Smith, "Botnet Attack Services on the Darknet."

discuss the benefits that come with having access to the dark web and present the argument that many users assert for its existence and unrestricted activities.

Positives of Anonymous Activity on the Dark Web

China has long been known for censoring its population's internet access and closely monitoring online activity. Interestingly, though China's constitution claims to give the right of freedom of speech and freedom of the press to its citizens, these freedoms are not often upheld and citizens can be subject to the arbitrary power of the government simply by being accused of exposing secrets or espionage. According to the Council on Foreign Relations, "It's tactics often entail strict media controls using monitoring systems and firewalls, shuttering publications or websites, and jailing dissident journalists, bloggers, and activists."[20]

The Hong Kong pro-democracy demonstrations are a great example of this. Several news sources reported how certain websites were blocked under the new national security law passed shortly after China gained control of the territory.[21] Other sources also reported concern over China's removal of pro-democracy books under the same law and their forced removal from bookshops, schools, and libraries.[22] As one might imagine, the Chinese government has an invested interest in keeping its citizens off the dark web as well, since they cannot control the information that Chinese users consume or spread. The Great Firewall of China, as it is known, does actively try to block entry relays to the Tor network.[23] However, Tor is constantly evolving to allow undetected access and regularly creates secret relays that are very difficult for the

[20] Beina & Albert, "Media Censorship in China."
[21] Soo, "Hong Kong Internet Firm Blocked Website."
[22] BBC, "Hong Kong Security Law."
[23] Emerging Technology from the arXiv, "How China Blocks Tor."

government to find and, subsequently, block. The same anonymity that covers the footprints of criminals and delinquents also works to hide and protect political dissidents in countries that would otherwise be inaccessible via the internet without harsh persecution.

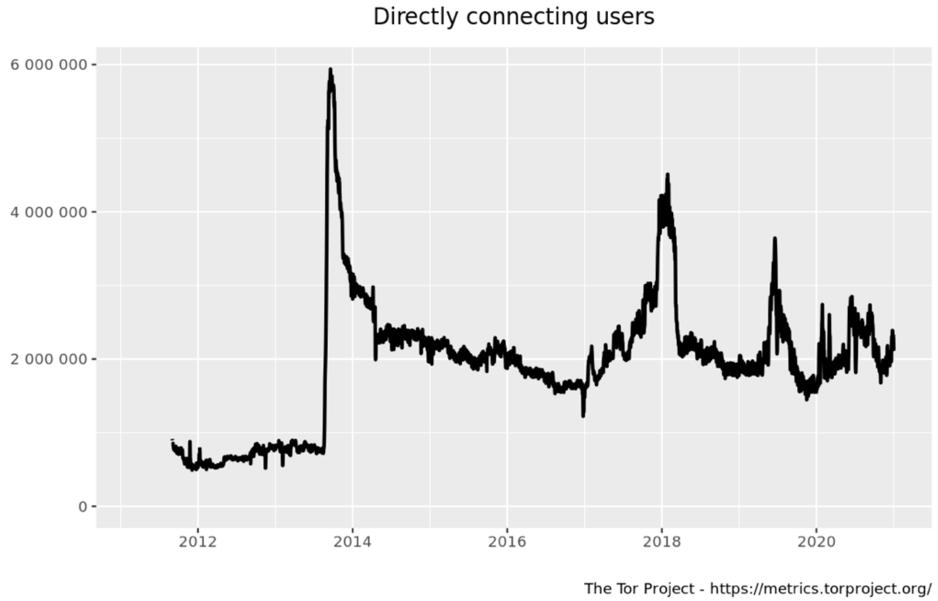
Though China is a guilty offender of censorship and maltreatment of dissenting voices, they are not alone in using these strategies to maintain control of their populations. With Google's uncontested rise to power as a monopoly on search engines and the political moves made by social media companies like Twitter and Facebook, even those in progressive countries have reason to question how dedicated private corporations are to the freedom of speech and exchange of ideas. Users of social media sites on the dark web report feeling a sense a freedom to know that they can discuss just about anything with other users. In one ethnographic study conducted by Robert W. Gehl, the author recalled being told by a user of Dark Web social media site, "If I want to talk about things illegal in my country or report some abuse I can without fear of retaliation."[24] This includes topics that are often taboo in our societies, such as controversial political views or suicide. This platform enables truly free speech, which then allows for the open exchange of ideas and facilitates discussion about topics that would otherwise be left to fester unchallenged.

In fact, there is a growing number of users flocking to the Tor browser. Though it might be intuitive to interpret this as the crime rate increasing, these new users are often after anonymity for yet another reason. Though uninhibited by political persecution or social ostracization, it is the lack of privacy and constant data collection imposed by many browsers and websites that is driving this movement. Internet users that would otherwise log into Facebook or do online shopping on the surface web are finding that they can download the Tor

[24] Gehl, "Power/Freedom on the Dark Web," 1232.

browser and use its cloaking feature to surf their normal websites without the fear of cookies being planted without their permission or having their shopping habits tracked, analyzed, and sold to other companies that might find their interests useful in targeted advertising. Though this fear might seem a little far-fetched or paranoid, a growing number of users are realizing that their innocent wanderings on the surface web do come at a cost.

Figure 2



The figure above shows the number of directly connecting users of the Tor browser between 2010 and 2021, generated and taken from the Tor metrics website. The huge spike around 2014 has been attributed to a botnet operation, so it can be ignored as an outlier.[25] However, even after the spike, we can see that the use of Tor has increased since 2014 and goes through periods of rapid growth before tapering off again. If experts are right about a mass

[25] Gehl, "Power/Freedom on the Dark Web," 1223.

exodus from the surface web to the dark web by ordinary people for privacy reasons, we should expect this figure to have another spike soon.

With both the benefits and the drawbacks laid out clearly, the burden is on the policymakers to decide how to balance the right of freedom of speech with the obligation to uphold the law. The Center for International Governance Innovation, a Canadian think tank, found that 71 percent of Americans would favor shutting down the dark web for good.[26] Though this would be virtually impossible without destroying the infrastructure that the surface web also uses to function, there has been talk of making attempts to restrict access or criminalize the use of the dark web. Very little guidance is offered to policymakers on how to approach this contentious topic. By analyzing this decision with the approaches used by utilitarians, libertarians, and Kantians, I will provide insight into how these obligations should be compared.

The Utilitarian Approach

For those who ascribe to a utilitarian ideology the maximization of happiness, also called utility, is the main focus and goal of every policy or action. Enchanted by the cleanness of the quantitative approach to social science that economists took, utilitarians sought to use similar methods in political science to determine what makes good policy. In practice, this means adding up the harms and the benefits that are caused by a particular topic or activity and weighing them against each other. If the net outcome is positive, then it is a good policy. If the net outcome is negative, then it would be a bad policy to implement.

[26] Greenberg, "Dark Web's Bad Rep."

The utilitarian approach is appealing for a couple reasons. To begin, the premise is easy to understand. Some might even say it is intuitive. If a certain policy will benefit fifty percent of the population and the rival policy will benefit eighty percent of the population and we assume the intensity of the benefits is equal, it seems clear that the policy benefitting eighty percent should be chosen. Despite its simplicity, however, the caveat of assuming the benefits are equally intense is important for utilitarian calculations. That is why it can be better to view this theory as maximizing utility instead of focusing solely on the sheer number of people benefitted. This means that if a certain policy only benefits a small minority group and slightly harms the majority group, it is not necessarily written off. Instead, we would have to compare the intensity of benefits. So, if the policy drastically improves the utility of the minority group and only slightly decreases the utility of the majority, it is still likely that a utilitarian would see this as a good policy. Though the highest percentage of people is not benefited, utility is still maximized.

However, the process of determining net utility can be slightly more complicated than it first appears. The utilitarian calculations can sometimes lead to the acceptance of actions that some might want to denounce as a matter of principle. Torture is viewed as morally repugnant in most societies, and many people oppose its use under any circumstances. However, if we have good reason to believe that torturing a suspected terrorist would allow us to locate the ticking time bomb that he planted somewhere in the city, thus saving a hundred lives, would it be morally justified? What if we could save thousands of lives? What about a million? If the answer changes depending on the number of lives saved, that means that torture can be morally justified in at least some situations[27]. Even those that reject torture on principle might find that,

[27] Sandal, "Justice," 38-40.

if enough harm could be mitigated, using it as a tactic in this situation would be considered ethical and we cannot discount its use based on an unchanging moral principle.

Utilitarianism is an important approach to evaluating policy questions and can provide a depth of analysis to the discussion of the dark web. For example, a helpful question to ask ourselves is if we were to sum the benefits that the dark web provides and subtract the sum of the negative consequences from that total, would we have a positive or negative amount of utility? Even with the objective benefits and drawbacks clearly delineated, it can be very subjective to quantify the disutility a victim experiences when having stolen passwords auctioned off on a dark market. Nevertheless, we can explore this question of quantifying the positives and negatives of the dark web with further discussion.

According to one study, "The most common uses for websites on Tor hidden services are criminal."[28] Another researcher stated that it was a "very conservative" estimation to say that half of the activity that takes place on the dark web is illegal.[29] This is indeed a disturbing trend, and we may become convinced that utilitarians would all agree that the drawbacks far outweigh the benefits. The conclusion based on this thinking, then, would surely be to restrict the dark web as tightly as possible. This, it could be argued, would be the best way to maximize utility.

However, as I mentioned above, simply adding up the existing utility to determine the best way forward does not always yield the anticipated clear path forward. Jeremy Bentham, the founder of utilitarianism, thought that we need to be careful in how we evaluate situations in which future consequences to the decision are left unaccounted for. In Michael Sandal's book *Justice: What's the Right Thing To Do?*, the author gives an illustration of the Roman practice of throwing Christians into an amphitheater filled with lions as entertainment. In the example, there

[28] Moore & Rid, "Cryptopolitik and the Darknet," 21.
[29] Shillito, "Untangling the Dark Web," 190.

are many people who benefit from this morbid entertainment, so their utility is very high. On the other hand, the Christians are suffering quite badly. But, because of their small numbers, their suffering does not outweigh the benefit that the Roman people get from this pastime. Would utilitarians really say that this is an acceptable practice, then?

The short answer is no, they may not. In taking into account every aspect that is necessary, a utilitarian may come to the conclusion that this practice is morally wrong because it could degrade a person's conscience enough to increase crime rates or, perhaps, eventually lead to mass fear from the viewers attending these events who wonder if they themselves may someday be thrown to the lions[30]. This would change the outcome of the calculation, making it so that utility would actually be maximized by outlawing such practices. So, for utilitarians, it is vitally important to take into consideration future utility when determining the best policy. Otherwise, we could end up with unexpected results that may seemingly justify genocide against a small minority in favor of entertaining the majority or equally strange conclusions.

For the dark web, this means that the calculation is a little more complicated than I originally presented it to be. Though we do have to weigh the pros and cons of what the current activity looks like on the dark web, we also need to take into account how that might change, as well as any additional details that might be less obvious yet crucial to the calculation. With this in mind, we can reframe the question of whether or not the benefits outweigh the drawbacks in the context of a broader range of considerations.

The fact presented earlier about the number of people who use the dark web for nefarious purposes remains. However, this may not necessarily mean that the overall utility is tipped in their advantage to make the whole operation negative. Consider the plight of a political activist

[30] Sandal, "Justice," 37.

in China or a freedom fighter in North Korea. These individuals, though the minority on the dark web, represent far more people than just themselves. The act of getting on the dark web from one of these countries can be challenging, so not every individual who wishes to speak up about the injustices they are witnessing are able to do so. Those that can are, in a sense, acting on behalf of many people who share their beliefs and desires. The utility of those that benefit from others having access to the dark web to share their stories needs to be taken into account as well. With the relatively small population that uses the dark web currently, it is not a stretch to imagine how this utility may, in fact, outweigh the problems caused by criminals or black-market customers.

Another prominent utilitarian thinker, John Stuart Mill, was a proponent for even further considerations when determining which route maximized utility. According to Mill, utility should not be maximized on a case-by-case basis, but rather overall with the long-term outcome as a focus.[31] With this in mind, consider the growing concern with online privacy violations and general worry associated with smartphones listening to their surroundings. There are many documented cases of smartphones or household devices listening to conversations and using the information mentioned to better target their constituents with relatable advertisements when venturing online.[32] In addition, social media companies and even search engines have been accused of selling private information collected from users without their knowledge or consent. More and more, online users are realizing that they are losing control over what information is being taken from them as they go about their business on the surface web.

Some people do not fear this reality, and others even embrace it. Targeted advertising may just mean more productive bouts of online shopping. For others, however, this is a breach

[31] Sandal, “Justice,” 50.
[32] Kröger & Raschke, “Is My Phone Listening In?” 115.

in privacy and a serious concern. Individuals in this camp are left with a choice: give up their online personas forever or trade their favorite web browser for one that allows them to navigate all their frequented sites anonymously. A growing number of people are beginning to choose the latter option. Without any intention of accessing content that is unique to the dark web, these users gladly interlope around the web on a browser like Tor for the sole purpose of protecting their privacy.

Mill would say that this growing platform of users deserves to be taken into account when determining the utility created by the dark web as well. Though in the short run these individuals are in the minority, it may not be long before we see this subset grow into a powerful majority. The requirement to take this long-run view into consideration furthers the case that utility would actually be maximized by keeping access to the dark web unrestricted to the general population. It may also be worth noting here that, despite the claims presented earlier that most dark web sites contain illegal or illicit material, this may not be a proper metric to use when assessing what users are going to the dark web for. In fact, it has been suggested that a mere 1.5% of users of the Tor browser are currently using it to access material on the dark web.[33] This is a difficult variable to measure simply because of the anonymity that Tor provides, but it is compelling nonetheless. If true, we may conclude that there are already enough people using these methods to protect their privacy that their utility outweighs the minority who are acting on bad intentions.

The last consideration to discuss before reevaluating our total utility is perhaps one of the most important. Mill was famous for many additions to utilitarianism, including higher and lower pleasures and his distaste for conformity. Mill is particularly well known, however, for his

[33] Thomas, "Is the Dark Web Going Commercial?"

views on free speech. According to him, the ability to openly deliberate opinions with fellow humans was so great that no speech could ever be justly curbed. This includes speech that is offensive or untrue. Social norms could be established to prevent certain topics from being discussed, but the topics themselves should not be restricted by any means in order to engage with each other and find truth through debate and discussion.

The dark web is, perhaps, the best example of this kind of environment. In doing an ethnographic study on dark web social media sites, Robert W. Gehl noted that the freedom to discuss otherwise taboo topics was reported to be an important tenant among the users. These communities still had moderators to remove posts that violated any of the few rules, such as posting nude photos of minors, but the community was mostly self-policing. Here, users felt comfortable discussing topics like suicide, self-harm, and controversial political opinions in an open environment with many other users to provide feedback and share experiences. Not only did this allow for users to feel heard, but it gave them a chance to hear other perspectives and think outside their own paradigm. Without a site to facilitate such discussion, this broadening of views could not take place. The surface web tries to facilitate discussion like this but restricts speech to the point that Mill would be uncomfortable. Facebook may have had the United States' best interest in mind when it chose to censor Donald Trump in the last few days of his presidency, but there are definitely concerning aspects of this decision that are not taken lightly by proponents of free speech.

So, with these discussions brought forth, I will re-present the case for how utilitarians would respond to the question of whether or not it is morally right to restrict access to the dark web. The consequences, as we have discussed, remain unchanged and present an enormous amount of disutility that is associated with the crimes that take place on the dark web. This includes the harm caused to society from illegal weapon purchases, the hiring of private hackers, and the degradation of victims of illegal pornography. These are serious negatives and should not be taken lightly.

Despite this, there are enormous advantages to allowing free access to the dark web as well, with the possibility of growing larger as a new subgroup begins to download and use the dark web with more innocent intentions. The combined utility of the political activists and those they represent, a growing number of users who desire to protect their privacy without intention of abusing anonymity, and the human benefit of free speech and deliberation create a massive counterweight to the harms listed above.

With the guidance of Mill's advocacy of the importance of freedom of speech being unrestricted and the increasing rules that surface web social media sites impose on their users, I believe that utilitarians would reject policies that impose restrictions on accessing the dark web. As law enforcement personnel improve their methods for tracking down notorious criminals on the dark web, we may even start to see the already small group of people wreaking havoc on society through the means provided by dark web browsers diminish further. This scale will inevitably continue to tip in the favor of allowing unfettered access for those who so desire it.

The Libertarian Approach

Another school of thought that we could examine is libertarianism. Those who ascribe to this ideology believe that human freedom is the most important value for society and should not be restricted under almost any circumstances. According to Sandal, the intellectual doctrine behind libertarianism came about in the 1960s. At that time, its primary purpose was to oppose the rising welfare state.[34] It was originally focused largely on economic policy, but it began to spread to other areas of governmental relations with citizens.

As one may surmise, libertarians prefer a government that has a minimal role in society and generally adopts a non-interventionalist philosophy. Robert Nozick, a well-known libertarian thinker, once wrote in the opening of his book *Anarchy, State, and Utopia* that, "a minimal state, limited to the narrow functions of protection against force, theft, fraud, and enforcement of contracts, and so on, is justified; that any more extensive state will violate persons' rights not to be forced to do certain things, and is unjustified; and that the minimal state is inspiring as well as right."[35]. This minimal state, then, cannot be paternalistic, legislate based on morals, or redistribute wealth or income.[36]

Though this ideology would seem to overwhelmingly favor the unrestricted public access to the dark web, I want to pause briefly to consider an argument against this position. The dangers of the dark web have been discussed in detail, and some may notice that both theft and fraud may, technically, take place on the dark web. Since part of the government's duty, according to Nozick, is to protect its citizens against such threats, perhaps there is some merit in the argument that libertarians could favor restrictions.

However, this argument falls apart when libertarian attitudes are more closely examined. Yes, the government should protect against theft, but that does not mean that it is personally responsible for setting a watchman outside every home to prevent a burglary. Similarly, it is not responsible for preventing individuals from accessing a website that *might* cause an inexperienced user to fall victim to a cybercrime. To a libertarian, this would be paternalistic.

[34] Sandal, "Justice," 61.
[35] Nozick, "Anarchy, State, and Utopia," ix.
[36] Sandal, "Justice," 60.

The government should not be able to tell a citizen that it knows what is in her best interest better than she does. If the user wishes to take the risk and visit the dark web without properly arming herself with knowledge and firewalls, that is her freedom to do so. Even if it may cause harm, that harm in itself is not the government's responsibility to protect at the expense of autonomy for the user.

Because of its fierce advocacy for freedom and against paternalism, the libertarians will always be in favor of keeping the dark web unrestricted. The notion that immoral actions take place there would pose no qualms for a libertarian. In their view, the government does not have the right to legislate based on morals.[37] So, even if a libertarian might find some of the activities that take place on the dark web to be depraved, that in and of itself is not enough to justify intervention.

In addition, due to other beliefs that libertarians hold, the dark web may not seem like such a nefarious place after all. Because of their view of the government's minimal role in society, most libertarians are of the opinion that it has no authority to make laws against the use of drugs or the possession of any kind of weapon. This includes highly addictive drugs and anti-aircraft missiles.[38] Instead of viewing the illegal purchase of drugs and weapons on the dark market as something that is harmful to society and only perpetuated by criminals, libertarians are more likely to be sympathetic to these individuals and label them as fighting against an unjust system. Because of this, the negative parts of the dark web that we identified in the section on utilitarianism would likely be viewed rather positively by libertarians. Those that are responsible for the dark markets can be seen as political dissidents instead of crooks.

[37] Sandal, "Justice," 60.

[38] Block, "Anti-aircraft Missiles and Gun Control," 77-80.

Libertarians, then, would join utilitarians in denouncing any governmental attempt to restrict access to the dark web. With their dedication to a minimal state and beliefs about the moral supremacy of human freedom, there would be no legitimate argument that could convince them that any regulations are merited. Libertarians would say that paternalism is a threat in and of itself and actions taken in its name should be highly scrutinized to protect individual liberty. Imposing restrictions on the dark web would not stand up to this scrutiny.

The Kantian Approach

The last school of thought that I will examine is that which was shaped by Immanuel Kant. Kant was born and raised in East Prussia in 1724. Despite coming from a family with modest means, he did well in school and eventually became a lecturer at an institute in the town he grew up in. He continued to teach there until retirement at the age of seventy-two.[39] During his time teaching, Kant began to publish several major works. His first, *The Critique of Pure Reason*, was a challenge to the empiricist theory of knowledge put forth by David Hume and John Locke.[40] After this, he turned his focus to critiquing utilitarianism as proposed by Jeremy Bentham. This book, called the *Groundwork for the Metaphysics of Morals*, asserted that utilitarianism was wrong for believing that we can determine what is ethical simply by maximizing happiness. Instead, Kant believed that there were certain rights that all men were inherently born with.

His philosophy revolved around the idea that we must treat ourselves and others not simply as a means to an end, but as an end in and of itself. This idea led him to conclusions such

[39] Rohlf, "Immanuel Kant."
[40] Sandal, "Justice," 104.

that murder, suicide, and the degradation of oneself or others is morally wrong and should be avoided. He also held very strong beliefs about lying. According to Kant, lying was never justified, even if the purpose was to spare someone from an unpleasant truth or shield someone from undeserved tragedies. The reasoning is as follows: if you fail to tell someone the truth in order to avoid hurting their feelings, you are not treating them as an end. Instead, you are sparing yourself discomfort at the expense of respecting their rationality.

As with libertarians, Kant held strong regard for freedom. His version of freedom, however, is different from what a libertarian would propose. To Kant, to be free means to act autonomously. We can only act autonomously when we are acting not based on impulse or to satisfy our "appetites," but rather when we are free of those restrictions and acting based entirely on our rationality[41]. His version of freedom places high regard on autonomy and believes that we should avoid restricting autonomy, lest we restrict the freedom that flows from it.

This philosophy has interesting implications when applied to the dark web. After all, much of the negative activity that takes place there could certainly fall under the category of degrading. There is abusive and illegal pornography, the ability to buy any kind of drugs imaginable, and the ability to hire hitmen to assassinate an enemy. Kant would object to all of these things as being morally reprehensible since it either restricts one's own autonomy or another's, and certainly does not respect an individual as an end in themselves. The type of pornography found on the dark web degrades its victims, and consuming it contributes to this effect. It also is a prime example of using a person or people as a means to an end rather than an end. Drugs appeal to our appetites, not to our rational desires, and hitmen are hired to murder, which permanently restricts its victim's autonomy.

[41] Sandal, "Justice," 109.

With all this laid out, it is tempting to say that Kant would absolutely be in favor of restricting access to the dark web. This could be based on an argument that the activities on the dark web degrade ourselves or others, or that crime restricts autonomy, or that the activities that take place there appeal only to our appetites and do not constitute a truly free choice. Regardless of which argument is taken, it seems reasonable to assume that Kant would draw the conclusion that accessing the dark web is immoral and can or should be restricted. However, I contend that Kant would actually draw the opposite conclusion. Though his stance on freedom and autonomy can be argued to favor the restrictions of the dark web, it is even more convincingly applied to the maintenance of free access to it by the public.

My argument is as follows. Just as humans are morally unjustified in restricting one another's autonomy, so the government is bound by the same rules. If the government chooses to impose restrictions on accessing the dark web, they are restricting our autonomy. Without this autonomy, we are unable to act freely. That action, then, would be dubbed immoral by those that accept Kant's philosophy.

There are objections that can be raised to this simple argument, however. For example, as we have already mentioned, criminal activity often restricts others' autonomy as well. If the dark web is a breeding ground for criminal activity, then the government would be justified in restricting it in order to preserve freedom for those that would otherwise be victims. Despite the fact that doing so would decrease the autonomy of users that would not end up being victims, there are legitimate and moral reasons to prevent people from accessing the dark web in order to ensure that others' autonomy is not affected by crime.

This is a valid concern, but I argue that Kant would believe this to be a different kind of restriction to autonomy. In other words, in one situation, the government is *directly* stepping in and restricting the autonomy of a user. The user in question may be intent on committing a crime, or they might be law-abiding citizens with a legitimate purpose for accessing content on the dark web. In the other situation, the government is *failing to prevent* a victim's autonomy from being restricted as they become a victim of some criminal on the dark web. This failure to prevent autonomy from being restricted is different from directing imposing restriction. Since we are trying to answer the question of whether or not it is morally acceptable to restrict access to the dark web for policy purposes and not whether or not going on the dark web is a good idea for individual users, we must consider the first case presented. The government does not have the right to directly restrict an individual's autonomy in this way.

Moreover, Kant was a huge proponent of free speech and emphasized its importance as a precondition to autonomous action. In fact, between private citizens, Kant was hesitant to place any restrictions on speech except that which would lead to the loss of "rightful possessions" due to defamatory remarks or breaches in contract.[42] This liberal view of speech provides individuals with the ability to explore topics with one another without depriving each other of innate or acquired rights. In her paper *A Kantian Conception of Free Speech*, author Helga Varden writes, "It is in part for this reason that the resulting Kantian position will defend citizens' constitutional right to free speech, understood as their right to discuss even the most controversial topics amongst themselves – through films, articles, the media, internet medium, and so on."[43]

However, this view extends further than just speech between private citizens. In his essay *What is Enlightenment?*, Kant explains that the restriction of free speech "violates the

[42] Varden, "A Kantian Conception of Free Speech," 49.
[43] Ibid.

sacred right of humanity"[44] and prevents the government from being able to govern effectively. In Kant's view, the criticism of its citizens is necessary for any ruling authority to ensure they are ruling well. If the right to speak out against authority is extinguished, Kant believes that the victims are twofold. The citizens have their humanity restricted, while the governing authority is reduced to an individual or a group of individuals who misunderstand their mission and end up ruling poorly as a result. [45]

The platform of free speech that the dark web provides, then, might be even seen as desirable to Kantian scholars. The principle of being able to speak out against unjust rulers– one of the most touted good deeds of the dark web– is sufficiently important to Kant's idea of good governance and human autonomy that it would be wrong to restrict its access. Though some governments may prefer their citizens to refrain from critiques, this is an unwise desire that would hurt its legitimacy.

Scholars of Kant may notice here that we have not yet touched on the categorical imperative that was central to Kant's definition of reason. When humans exercise "pure, practical reason," we are acting from either a hypothetical imperative or a categorical imperative. A hypothetical imperative is conditional. It says that if we desire a certain outcome, we must take a certain action.[46] For example, if I want to receive a good grade in a class, I should study. This shows that studying is a good method to meet my desire, but it does not show whether or not studying is good for its own sake. On the other hand, the categorical imperative is unconditional. It is a basis of reason that is always true and good in and of itself. Kant writes, "It has to do not with the matter of the action and what is to result from it, but with the form and

[44] Kant, "What is Enlightement?", 8:39.
[45] Varden, "A Kantian Conception of Free Speech," 50.
[46] Sandal, "Justice," 119.

principle from which the action itself follows; and the essentially good in the action consists in the disposition, let the result be what it may."[47] According to Kant, this is the only imperative that has moral weight.[48]

As for what the categorical imperative actually tells us, Kant has two ways of framing the principle. Both are fascinating, but one is rather more helpful to my comparison of the dark web, so we will focus on that. The first understanding of the categorial imperative is as follows: "Act only in accordance with that maxim through which you can at the same time will that it become a universal law."[49] So, when we take an action, one way to determine whether or not it was moral or immoral is to ask ourselves whether or not we think everyone should act likewise. For example, if I were to steal some food because I forgot to pack myself a lunch for the day, I should ask myself if I think the principle I'm acting on can be universalized. How would society function if everyone decided to steal when it was convenient? If I cannot universalize the maxim, I should note that the action I was about to take is not moral.

This categorical imperative can be helpful for our understanding of why Kant would not be in favor of restricting access to the dark web. To understand why, we should ask ourselves what maxim we are purporting when we claim that the government should create policy that restricts access to the dark web. One answer would be that the government should create policy to protect its citizens against anything that it deems to be unsafe. This is, at its core, paternalistic. However, Kant rejects the notion that the state should act paternalistically at all. He believes that the state does not have the right to tell its constituents what is good and will lead to happiness, for to do so would be to treat them like children.[50] He wrote, "A government

[47] Kant, "Groundwork of the Metaphysics of Morals," 4:416.
[48] Sandal, "Justice," 119.
[49] Kant, "Groundwork of the Metaphysics of Morals," 4:421.
[50] Stanford Encyclopedia of Philosophy, "Kant's Social and Political Philosophy."

established on the principle of benevolence toward the people like that of a *father* toward his children - that is, a *paternalistic government* in which the subjects, like minor children who cannot distinguish between what is truly useful or harmful to them, are constrained to behave only passively, so as to wait only upon the judgment of the head of state as to how they *should be* happy and, as for his also willing their happiness, only upon his kindness - is the greatest *despotism* thinkable (a constitution that abrogates all the freedom of the subjects, who in that case have no rights at all)."[51] Because Kant would reject the principle that stems from the universalization of the maxim, we can reject that the policy would be acceptable as a categorical imperative.

An Ethical Way Forward

Now that we have examined the policy goal of restricting access to the dark web from the perspectives of utilitarianism, libertarianism, and Kantianism, I will draw some conclusions from the discussion. To begin, all three schools of thought arrive at the same conclusion: it would be morally wrong to prohibit or restrict access to the dark web. The reasoning behind each conclusion is different, of course, but the final judgement remains unanimous.

To an extent, we must take into consideration that some of the analysis done was subjective. Though utilitarians like to deal in absolutes, it is impossible to decide on a scale that everyone agrees upon in determining how harmful or beneficial an activity is. Similarly, with Kant's philosophy, it is feasible that someone could argue against my autonomy principle and state that Kant would be opposed to many things that happen on the dark web and would find it

[51] Kant, "On the common saying: That may be correct in theory, but it is no use in practice," 8:290-291.

morally justified to restrict access regardless of the limitations this could pose on freedom. Despite these objections, I have argued what I believe to be the most compelling interpretations of the three paradigms and maintain that those objections were thoughtfully considered in each section.

If I am correct and restricting access to the dark web is an immoral objective for policymakers to pursue, we must ask ourselves what our options are moving forward. With so many people in favor of shutting the dark web down in an attempt to curb the negative effects associated with it, it seems wrong to drop the topic entirely without any attempt to rectify the morality of the issue with the opinion of the majority. Fortunately, we are not without options here. Though the dark web is designed to make tracing individuals and their activities impossible, some experts have weighed in on potential ways to mitigate the societal consequences that are associated with the dark web.

The FBI has developed tools that can aid them in bringing criminals that use the dark web as a cloak of anonymity to justice. One of these tools is a computer and internet protocol address verifier that can actually flag Tor traffic separately from normal traffic that bounces through internet routers.[52] Though this does not unmask the criminals, it can be helpful in narrowing the scope of the investigation to a smaller geographical area. Another tool, called Memex, was developed by the Defense Advanced Projects Research Agency in 2015 and is more recently making itself a staple in law enforcement strategies on the dark web. Though it, too, cannot destroy the anonymity of users, it can flag illegal content and create a database that collects and stores these trends for analysis.[53] With the continuous advancements in big data analysis, these databases are invaluable assets to analyzing trends in where and what is happening on the dark

[52] Chertoff, “A public policy perspective on the Dark Web,” 34.
[53] Otto, “Memex.”

web. Together, tools like this are making it possible for law enforcement to intervene in illegal and harmful activity that takes place on the dark web without disturbing the anonymous activities of its innocent users.

Another route that law enforcement has had success with is keeping track of usernames on dark web accounts that are engaging in illegal activity and monitoring for the same usernames on the surface web or waiting for some type of identifiable information to be slipped innocuously. Though criminals try to be careful not to link any dark web profile to their surface web activities, humans are all fallible and have limited memory capacity. Reusing passwords and usernames is a fault that nearly everyone falls into eventually for the sake of keeping track of accounts. If the operation has been going on for long enough, complacency slips in and the need to remember a username supersedes the need to keep a distinct separation from dark web operations and surface web activities.

Perhaps one of the most famous examples of this strategy being used was the international collaboration known as Operation Bayonet. Working together with law enforcement in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, France, and Interpol,[54] the FBI was able to take over AlphaBay, the largest black market on the dark web, and not only successfully arrest the administrators that ran the site, but also hundreds of people buying illegal substances from it.

AlphaBay was the successor for the famous Silk Road black market. After the owner of the Silk Road was arrested and convicted for his part in operating a site that allowed for the buying and selling of illegal drugs, previous users of the Silk Road were desperate to find somewhere new to purchase these commodities. There were a couple other options available,

[54] Office of Public Affairs, "AlphaBay Shut Down."

though much smaller than the Silk Road. AlphaBay was one of these options. It very quickly saw a rise in popularity with the shutdown of the Silk Road and subsequent disappearances of other markets such as Evolution. Naturally, this caught the FBI's attention. They began to assign undercover agents to create user accounts and purchase drugs, credit card skimmers, and other illegal goods off of the marketplace to see if they could find any incriminating evidence through this probing.

This strategy was not successful at first. Though they were able to find out that the drugs were being shipped from California, they still had no way of narrowing down exactly who was behind the operations. That is, until one agent decided to sign up for a new account and start fresh. This agent was greeted by an email welcoming him to the site, but unlike previous correspondence, this email listed a reply address in the header for a Hotmail account. The FBI immediately jumped on this information and wasted no time in connecting the email account to a LinkedIn profile. After this, they were quickly able to identify the owner as Canadian-born Alexandre Cazes and track down his whereabouts. Cazes was living in Thailand despite the server being located in Canada.[55] Their plan was to cause a disturbance outside his home while he was working on his computer so that they could lure him away without logging out. Their goal was to arrest him and gain access to the account that he used to run AlphaBay.

The FBI was able to successfully accomplish this feat by driving into his front gate with a car and creating a scene with onlookers. When Cazes raced out of his home to investigate, he was seized. His account, which was left open on his computer due to the unexpected disruption, was confiscated by the US government.[56] The FBI then proceeded to run AlphaBay through this account as if nothing had happened. News of his arrest was kept quiet so as to not alert users of

[55] FBI, "AlphaBay Takedown."

[56] Franceschi-Bicchierai, "FBI Shows Arrest Video."

AlphaBay that anything had changed. However, shortly after his arrest, Cazes committed suicide in a Thai prison and the news broke of AlphaBay's compromise. This led to a flood of users going to the next most popular dark market: the Hansa Market. Unbeknownst to the users, however, Hansa had recently been taken over by the Dutch government in a similar operation.[57] This allowed the Dutch law enforcement to trick users into downloading and running scripts that would, essentially, send out beacons to reveal their locations. This led to many more arrests and charges.

A last consideration is more preemptive than the methods discussed previously. Consider this: why do criminals go on the dark web to begin with? For the most part, it is because they are intelligent enough to know that their activities can be traced back to them relatively easily on the surface web. However, there are a surprising number of people with bad motives that are not aware of this fact. A majority of internet users could not define what the internet is or how it works; they are more likely to identify the internet as being their favorite browser than to identify any protocols or structures that the internet is based upon. This can be a serious advantage to law enforcement personnel. Perhaps one of the best strategies we could adopt, then, is to prevent the illegal activities from being pushed to the dark web in the first place. Though there are certainly moral qualms associated with allowing a human trafficking website to remain of the surface web for easy access to anyone, the benefits to law enforcement attempting to track down the instigators is significant. Ultimately, there may need to be a line drawn somewhere as to what is okay to leave on the surface web and what is not, but the more websites that we overtly censor, the more we will have slipping to the dark web where we cannot easily trace origins.

[57] Office of Public Affairs, "AlphaBay Shut Down."

So, though direct restriction of the dark web may not be a good policy to pursue, we are finding ways to still target the illicit and illegal happenings of the dark web while leaving the rest of its users protected. In all of the cases listed previously, the anonymity of the dark web is never jeopardized. Instead, human error and slip-ups are the causes behind these criminals being located and brought to justice. Tools like Memex and the computer and internet protocol address verifier are both keys to narrowing down where the crime is conducted, but clever law enforcement tactics like those seen during Operation Bayonet are crucial in being able to prevent serious harms from persisting under the cloak of anonymity that the dark web provides.

Conclusion

Over the years, the dark web has garnered fierce opposition and support for its existence. The harms that have been brought about by its activities have left many victims wanting justice, or at least greater restrictions on who can access it and how. This desire is merited, but those in charge of policymaking on this frontier need to be careful to assess the whole range of risks and benefits that come with the dark web's existence. This paper attempts to guide policymakers on the best policy going forward.

Though the majority of the population in the United States and some other countries believe that the dark web should be shut down, this is an unrealistic policy to pursue. As long as there is one computer owner that is sympathetic to the causes of the dark web, there will always be a volunteer node through which to route traffic. The only way to effectively shut down the dark web would be to destroy the infrastructure that makes it possible. To do so, however, would be to destroy the infrastructure of the surface web as well. The best policymakers could do to prevent all risk associated with the dark web, then, would be to attempt to restrict public access. Other countries have attempted this with moderate success, but dark web browsers are constantly evolving to undermine these policies.[58]

Nevertheless, it is important to do more than just assess whether or not the policy would be possible. As technology advances, we may find that it is no longer a stretch to believe that the dark web could be effectively restricted. We also need to ask ourselves whether or not it is morally justified to restrict access to the dark web. There are good arguments on both sides of the debate, but I have shown that utilitarianism, liberalism, and Kantianism would all reject the policy of restricting access to the dark web as immoral.

Utilitarianism would reject the policy of restricting access to the dark web on the grounds that it would, ultimately, decrease the overall utility of users and non-users alike. Though restricting access to the dark web would prevent disutility caused by crimes that take place there, it would come at the cost of forums for truly free speech. This would affect political dissidents and freedom fighters in countries that have extreme censorship laws as well as individuals who wish to have nearly unmonitored forums to exchange controversial ideas that would otherwise be removed or restricted. As the number of people concerned about privacy on the surface web increases, there will also be a rise in users with no ill intent that use browsers like Tor simply to mask their identities to protect their privacy.

Libertarianism would reject the policy of restricting access to the dark web because they believe that the only acceptable reason for the government to interfere in a person's freedom is to prevent force, theft, fraud, and to enforce contracts. This belief in the minimal state leads libertarians to have a very strict view on impediments to freedom. Paternalistic policies are

[58] Emerging Technology from the arXiv, "How China Blocks Tor."

frowned upon and restricting the dark web to the public for their own good would certainly be considered paternalistic.

Kantianism would reject the policy of restricting access to the dark web because of their strict belief in autonomy and the role it plays in freedom. Though crime does restrict the autonomy of the victim, the failure to prevent the crime from taking place is indirect. On the other hand, the government's role in preventing people from accessing the dark web is a direct infringement on autonomy. Though Kant would object to many things that take place on the dark web, he would reject the notion that restricting access to it would be a morally good policy to pursue.

I have shown that three prominent political philosophies converge on the conclusion that restricting access to the dark web is morally wrong. This is not a policy that we should pursue. Instead, we should continue to allow unfettered access while also pursuing creative law enforcement techniques to curb crime that takes place on the dark web. We should also continue to develop tools like Memex that do not interfere with the anonymity of the dark web but can give law enforcement an extra edge on tracking down criminal operations and, combined with other intelligence, may lead to charges and arrests. We should also try to prevent crime from being driven to the dark web by allowing a certain amount of illegal activity to exist on the surface web, where law enforcement can more easily trace the perpetrators and prove their association with the crime in question.

Bibliography

"AlphaBay Takedown." FBI. July 20, 2017. Accessed March 15, 2021. https://www.fbi.gov/news/stories/alphabay-takedown.

Bergman, Michael K. "White Paper: The Deep Web: Surfacing Hidden Value." *The Journal of Electronic Publishing*7, no. 1 (August 2001). Accessed March 16, 2021. doi:https://doi.org/10.3998/3336451.0007.104.

Block, Walter. "Anti-aircraft Missiles and Gun Control." *Journal of Social and Administrative Sciences*3, no. 2 (June 2016): 77-82. Accessed April 8, 2021. http://kspjournals.org/index.php/JSAS/article/view/827/947.

Chertoff, Michael. "A Public Policy Perspective of the Dark Web." *Journal of Cyber Policy*2, no. 1 (March 13, 2017): 26-38. Accessed February 23, 2021. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1298643?needAccess=true

Emerging Technology from the ArXiv. "How China Blocks the Tor Anonymity Network." MIT Technology Review. April 04, 2012. Accessed March 15, 2021. https://www.technologyreview.com/2012/04/04/186902/how-china-blocks-the-tor-anonymity-network/.

Franceschi-Biccheirai, Lorenzo. "FBI Shows Arrest Video Of Dark Web Kingpin Who Died By Suicide in Police Custody." VICE. January 10, 2018. Accessed March 15, 2021. https://www.vice.com/en/article/59wwxx/fbi-airs-alexandre-cazes-alphabay-arrest-video.

"GCHQ to Help Tackle 'dark Net' Child Abuse Images." BBC News. December 11, 2014. Accessed March 9, 2021. https://www.bbc.com/news/uk-30426164.

Gehl, Robert W. "Power/freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network." *New Media & Society*18, no. 7 (2018): 1219-235. Accessed January 20, 2021. doi:10.1177/1461444814554900.

Greenberg, Andy. "Dark Web's Got a Bad Rep: 7 in 10 People Want It Shut Down, Study Shows." WIRED. March 29, 2016. Accessed March 17, 2021. https://www.wired.com/2016/03/study-finds-7-10-people-want-dark-web-shut/.

"Hong Kong Security Law: Pro-democracy Books Pulled from Libraries." BBC News. July 05, 2020. Accessed March 10, 2021. https://www.bbc.com/news/world-asia-china-53296810.

Jacobson, Douglas. *Introduction to Network Security*. Boca Raton, FL: CRC Press, 2009.

Jardine, Eric. "Privacy, Censorship, Data Breaches and Internet Freedom: The Drivers of Support and Opposition to Dark Web Technologies." *New Media & Society*20, no. 8 (2018): 2824-843. Accessed September 4, 2019. https://journals.sagepub.com/doi/pdf/10.1177/1461444817733134.

Kant, Immanuel. *Groundwork of the Metaphysics of Morals*. Cambridge: Cambridge University Press, 1998.

Kant, Immanuel. "On the Common Saying: That May Be Correct in Theory, but It Is No Use in Practice." In *Practical Philosophy by Immanuel Kant*, 8:290-291. Cambridge: Cambridge University Press, 1996.

Kröger, Jacob Leon, and Philip Raschke. *SpringerLink*. Proceedings of IFIP Annual Conference on Data and Applications Security and Privacy, Charleston. June 11, 2019. Accessed March 18, 2021. https://link.springer.com/chapter/10.1007/978-3-030-22479-0_6#enumeration.

Moore, Daniel, and Thomas Rid. "Cryptopolitik and the Darknet." *Survival: Global Politics and Strategy* 58, no. 1 (February 1, 2016): 7-38. Accessed March 17, 2021. doi:10.1080/00396338.2016.1142085.

Murray, Andrew. "The Dark Web Is Not Just for Paedophiles, Drug Dealers and Terrorists." The Independent. December 12, 2014. Accessed March 9, 2021. https://www.independent.co.uk/voices/comment/dark-web-not-just-paedophiles-drug-dealers-and-terrorists-9920667.html.

Nancy. "The Dark Web: A History Lesson." Hack Ware News. May 18, 2019. Accessed March 3, 2021. https://hackwarenews.com/the-dark-web-a-history-lesson/.

Office of Public Affairs. "AlphaBay, the Largest Online 'Dark Market,' Shut Down." The United States Department of Justice. December 11, 2017. Accessed March 15, 2021. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

Otto, Greg. "Memex: Law Enforcement's Answer to Searching the Dark Web." FedScoop. February 14, 2015. Accessed March 15, 2021. https://www.fedscoop.com/memex-law-enforcements-answer-to-searching-the-dark-web/.

Owen, Gareth, and Nick Savage. "The Tor Dark Net." *Global Commission on Internet Governance*, 20th ser. (September 2015): 1-9. Accessed March 16, 2021. https://www.cigionline.org/sites/default/files/no20_0.pdf.

Plato. "Book II." In *The Republic*, 360c. Translated by Benjamin Jowett. Internet Classics Archive. Accessed March 10, 2021. http://classics.mit.edu/Plato/republic.3.ii.html.

Rauscher, Frederick. "Kant's Social and Political Philosophy." Stanford Encyclopedia of Philosophy. September 01, 2016. Accessed March 19, 2021. https://plato.stanford.edu/entries/kant-social-political/.

Rohlf, Michael. "Immanuel Kant." Stanford Encyclopedia of Philosophy. July 28, 2020. Accessed March 17, 2021. https://plato.stanford.edu/entries/kant/.

Sandel, Michael J. "The Greatest Happiness Principle/ Utilitarianism." In *Justice: What's the Right Thing To Do?*, 31-57. New York, NY: Farrar, Straus and Giroux, 2009.

Shillito, Matthew Robert. "Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law." *Information & Communications Technology Law*28, no. 2 (2019): 186-207. Accessed January 18, 2021. https://doi.org/10.1080/13600834.2019.1623449.

Smith, Daniel. "Malware and Botnet Attack Services Found on the Darknet." Radware Blog. July 13, 2016. Accessed March 18, 2021. https://blog.radware.com/security/2016/07/malware-and-botnet-attack-services-found-on-the-darknet/.

Soo, Zen. "Hong Kong Internet Firm Blocked Website over Security Law." AP NEWS. January 14, 2021. Accessed March 12, 2021. https://apnews.com/article/technology-beijing-internet-service-providers-democracy-hong-kong-9b004df447df043ecc7abc044edb2d15.

Tamburro, Paul. "You Are Being Watched: Terrifying Deep Web Footage Will Make You Afraid of Your Webcam." Mandatory. August 8, 2017. Accessed April 08, 2021. https://www.mandatory.com/living/1308371-watched-terrifying-deep-web-footage-will-make-afraid-webcam.

Thomas, Khristal. "Is the Dark Web Going Commercial? Internet Censorship May Be Driving the Trend." Georgetown Public Policy Review. March 6, 2020. Accessed March 16, 2021. http://gppreview.com/2020/03/06/dark-web-going-commercial-internet-censorship-may-driving-trend/.

Varden, Helga. "A Kantian Conception of Free Speech." *The Philosophical Foundations of Law and Justice*3 (2010): 39-55. Accessed March 20, 2021. https://philarchive.org/archive/VARAKC-5v1.

Weimann, Gabriel. "Going Dark: Terrorism on the Dark Web." *Studies in Conflict & Terrorism*39, no. 3 (December 22, 2015): 195-206. Accessed January 6, 2021. doi:10.1080/1057610X.2015.1119546.

"What Is The Dark Web & How Does It Work?" SecureTeam. March 11, 2020. Accessed March 16, 2021. https://secureteam.co.uk/articles/what-is-the-dark-web/.

Xu, Beina, and Eleanor Albert. "Media Censorship in China." Council on Foreign Relations. February 17, 2017. Accessed March 9, 2021. https://www.cfr.org/backgrounder/media-censorship-china.