12-15-2018

Web of Lives: How Regulating the Dark Web Can Combat Online Human Trafficking

Christopher Campbell

Follow this and additional works at: https://digitalcommons.pepperdine.edu/naalj

Part of the Criminal Law Commons, First Amendment Commons, Internet Law Commons, and the Sexuality and the Law Commons

Recommended Citation

Available at: https://digitalcommons.pepperdine.edu/naalj/vol38/iss2/4

This Comment is brought to you for free and open access by the School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Journal of the National Association of Administrative Law Judiciary by an authorized editor of Pepperdine Digital Commons. For more information, please contact josias.bartram@pepperdine.edu, anna.speth@pepperdine.edu.
Web of Lives: How Regulating the Dark Web Can Combat Online Human Trafficking

By Christopher Campbell

I. INTRODUCTION .................................................................................................................. 137
II. EVOLUTION OF COMBATTING ONLINE HUMAN TRAFFICKING ..................................... 138
   A. The History of Relevant Internet Laws ............................................................................. 139
   B. The History of Human Trafficking Laws ......................................................................... 141
   C. Present Human Trafficking Laws With Internet Regulation Implications ....................... 141
   D. Potential Future Online Human Trafficking Regulations ............................................. 142
   E. The Three Tiers of the Internet ....................................................................................... 144
   F. Effectiveness of Current Investigation and Prosecution of Human Trafficking .................. 146
III. ISSUES WITH SESTA AND SIMILAR LAWS ..................................................................... 148
   A. Prosecutorial Preference to Not Use Human Trafficking Laws ....................................... 148
   B. Why SESTA and Similar Laws Have Negative Consequences ....................................... 149
IV. ADDRESSING THE OTHER TWO INTERNET REGULATION PROPOSALS ............................ 151
   A. The Mens Rea Proposal is an Inadequate Internet Regulatory Scheme .............................. 151
   B. The Nonregulatory Proposal is an Inadequate Internet Regulatory Scheme ................... 152
V. PROPOSED LAW TO REGULATE THE DARK WEB .............................................................. 153
   A. Types of Dark Web Restrictions ................................................................................. 154
   B. More Stringent Sentencing for Criminals in the Dark Web .......................................... 158
   C. Four Calculated Proposed Methods to Combat Online Human Trafficking ................... 162
      1. Calculating the Ideal Proposal to Appropriately Combat Online Human Trafficking ....... 162
      2. Governmental Total Ban of the Dark Web (Total Ban) ................................................ 164
      3. New Dark Web-Human Trafficking Intertwined Statutes (Intertwined Statutes) ............ 166
      4. No Government Change (No Change) ......................................................................... 168
      5. New Criminal Dark Web Statute that Attaches to Previously Existing Human Trafficking Statutes (An Attaching Criminal Dark Web Statute) ................ 173
      6. An Attaching Criminal Dark Web Statute is the Most Effective Proposal ................... 175
   D. Potential Constitutional and Jurisdictional Issues with an Attaching Criminal Dark Web Statute .......................................................................................................................... 177
      1. First Amendment Concerns ....................................................................................... 177
      2. Jurisdictional Concerns ............................................................................................ 179
VI. CONCLUSION .................................................................................................................... 180
I. INTRODUCTION

A dream opportunity turned into a living nightmare for one young model. In the summer of 2018, British model Chloe Ayling was lured into a fake photoshoot and kidnapped by a group called “The Black Death” to be sold in the dark web.\(^1\) This incident demonstrates three important issues: 1) there are groups and individuals who have intricate online human trafficking\(^2\) operations on the internet, 2) no one is safe from being a victim of online human trafficking, and 3) catching online traffickers and dealing with online human trafficking is a very difficult process. There are international and domestic laws that prohibit online human trafficking and prosecute offenders, but generally, there are not a lot of human trafficking cases.\(^3\) One of the reasons human traffickers are not prosecuted is that traffickers are able to hide and operate in the Dark Web\(^4\) where it is challenging to

---

\(^1\) Matthew 22: 35–40. Thank you to all those who loved and supported me throughout law school: My dad and mom, my brother, Michelle S., my family at CCU and Cornerstone, and my friends and professors at Azusa Pacific University and Pepperdine Law.


\(^3\) There are various authors and articles which slice sex trafficking as a separate issue from human trafficking. The original idea for this article was to solely address sex trafficking because of its recent concern in the public sphere; however, sex trafficking is under the giant umbrella of the illegal concept of human trafficking. Though sex trafficking may be addressed, there is still the issue for those who are trafficked in other ways. For this reason, this article focuses on methods to combat human trafficking in general rather than specifically sex trafficking. Additionally, as this article discusses proposed methods to regulate the Dark Web, the focus is still to address human trafficking, but the ultimate proposed, ideal model can be applied to other types of crimes and laws.

\(^4\) Amy Farrell et al., *New Laws But Few Cases: Understanding the Challenges to the Investigation and Prosecution of Human Trafficking Cases*, CRIME L. & SOC. CHANGE, 140, 151 (2013). On average 71.5% identified sex traffickers are not charged with a state crime, and 49.25% of those identified as sex traffickers are not charged with a federal crime. *Id.*

\(^4\) There are instances in this article when the phrase “on the Dark Web” seems to be the more appropriate description of the situation; however, for the sake of consistency “in the Dark Web” was used uniformly throughout this article.
identify them. Therefore, in order to address the evolving concern of internet crimes, specifically online human trafficking, regulation of the Dark Web is necessary. This article argues that one of the ways to appropriately fight online human trafficking is through governmental regulation of the Dark Web. Specifically, this article argues that a new Attaching Criminal Dark Web Statute is the best method to combat human trafficking because it can incentivize prosecutors to use current human trafficking statutes to prosecute traffickers. This proposal can deter traffickers from enslaving people. Additionally, this article shows the evolution of online human trafficking laws, investigation, and prosecution (Section II); demonstrates why current and proposed laws do not effectively address the online human trafficking issue (Sections III and IV); introduces novel, proposed laws and methods to regulate the Dark Web (Section V); and presents arguments for and against proposals to regulate the Dark Web (V and VI).

II. Evolution of Combating Online Human Trafficking

One of the interesting aspects of online human trafficking enforcement and law is that it is a new area of policy. The recognition of human trafficking laws is a new development for the world. Also, internet law is a new and evolving concept, which at times piggybacks on communication, privacy, economic, and freedom of expression laws. Specifically, the concept of online human trafficking laws is extremely new since they are a combination of two non-traditional areas of the law which are fairly

---

6 See infra notes 7–26 and accompanying text.
7 A novel statute that is easy to read and apply, which ultimately can be an additional charge that prosecutors can use when a human trafficker uses the Dark Web specifically to traffic an individual, in addition to the human trafficking charge.
8 Farrell, supra note 3, at 140.
new and continuing to grow: internet and human trafficking law. To effectively combat online human trafficking, it is beneficial to understand the history of and present-day internet and human trafficking laws, and to discuss the potential future of online human trafficking laws and regulations.10

A. The History of Relevant Internet Laws

Before Congress enacted laws which governed and regulated internet use, the courts applied common-law principles to internet issues.11 Congress’ passage of the Communications Decency Act of 1996 (CDA) was one of the first instances of internet regulation in the United States.12 One reason Congress enacted the CDA was to protect children from obscenity on the internet and to ensure website owners would not be prosecuted for the content website users and visitors published on the website.13 Also, Congress passed § 230 of the CDA, which states that no “provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”14

10 Throughout this article, the mindset, opportunities, costs and risks, and benefits of a criminal are analyzed with a cost-benefit analysis approach. This approach consists of evaluating a situation and the likely outcomes a criminal may take determinant on a cost-benefit analysis. San José Univ. Dep’t of Econ., An Introduction to Cost Benefit Analysis, http://www.sjsu.edu/faculty/watkins/cba.htm (last visited Feb 5, 2018). Though this means a lot of speculation, the speculated courses of actions are rational. It is important to work off of these hypothetical potential courses of actions for policy making in order to better understand how the law contributes to the behavior of a criminal taking into account a cost-benefit analysis of their actions. Id.
12 Silvano, supra note 9, at 383.
This law protects website owners from any criminal and civil liability that could result from their users posts on their websites.\textsuperscript{15} Another reason Congress enacted the CDA was to promote the free market on the internet.\textsuperscript{16}

Additionally, federal and state laws allow governments to prosecute criminals who use computers or the internet to commit a crime.\textsuperscript{17} For example, the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, prohibits seven different acts using computers or the internet including the following: procurement of information that is of national security, compromising confidentiality, trespassing a government computer, accessing a computer to defraud and attain value, damaging information or a computer, trafficking passwords, and threatening damage to a computer.\textsuperscript{18} For California specifically, Penal Code § 502, the California Computer Data Access and Fraud Act (CDAFA), states it is a crime for someone who

\begin{quote}
[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.\textsuperscript{19}
\end{quote}

The State provision also criminalizes access and alterations to computers, data, programs, and alike without authorized access.\textsuperscript{20} Later in this discussion, these computer fraud laws are examined to

\textsuperscript{15} Silvano, \textit{supra} note 9, at 387.
\textsuperscript{16} Asención, \textit{supra} note 5, at 245. \textit{See also} Reno v. ACLU, 521 U.S. 844, 868–81 (1997); § 230. \textit{Note}, \textit{Reno} was declined to be extended in \textit{Moberg} v. \textit{33T LLC}, 666 F. Supp. 2d 415, 2009 U.S. Dist. LEXIS 93402, *10, 92 U.S.P.Q.2D (BNA), but the purpose of \textit{Reno} in this specific sentence is to demonstrate the judicial recognition of the importance of the CDA and not as an argumentative source.
\textsuperscript{17} \textit{See generally} 174 A.L.R. Fed. 101 (Originally published in 2001); 87 A.L.R. 6th 1 (Originally published in 2013).
\textsuperscript{18} \textit{See generally} 18 U.S.C. § 1030 (1986).
\textsuperscript{19} CAL. PENAL CODE § 502 (West 2016).
\textsuperscript{20} \textit{Id.}. 
decide whether they criminalize the changing of an IP address in
order to conceal the identity of someone who wishes to commit a
crime.21

B. The History of Human Trafficking Laws

The prosecution of human traffickers is a new development in the
law.22 Before the development of the current laws in place, human
traffickers were prosecuted for crimes that were already recognized,
such as kidnapping, assault, battery, slavery, fraud, and extortion.23
However, the penalties for these crimes were “weak and the statutory
language commonly characterizes victims as complicit.”24 In order
to address this issue, Congress enacted the Victims of Trafficking
and Violence Protection Act Of 2000 (“TVPA”).25 Since TVPA was
enacted, all 50 states have passed legislation that enables prosecution
and punishment of sex traffickers.26

C. Present Human Trafficking Laws with Internet Regulation
Implications

At the federal level, 18 U.S.C. § Pt. I, Ch. 77 sections 1581
through 1597 deal with human trafficking crimes and issues.
Additionally, in a series of legislation encompassed under the Justice
for Victims of Trafficking Act of 2015 (JVTA), Congress passed the
Stop Advertising Victims of Exploitation Act of 2015 (SAVE Act),
in order to amend 18 U.S.C. § 1591 to make it criminal to “advertise”
sex trafficking exploits.27 Additionally, 18 U.S.C. § 2251 is another
Federal law which criminalizes human trafficking of children.28
Through case law, the Fifth Circuit used three different opinions to

21 See infra Section (V)(C)(4).
22 Farrell, supra note 3, at 140.
23 Id.
24 Id.
26 Id. at 141.
27 Critics, Supporters at Odds Over Section 230 Change Aimed at Curbing Sex Trafficking, WASH. INTERNET DAILY, available on Lexis Advance (2017). 18
hold that those who trafficked children for sex are strictly liable for their crimes.\textsuperscript{29} However, in general, website owners are still protected and cannot be liable for their users' content on the website because of the protections afforded to website owners in § 230 of the CDA.\textsuperscript{30} However, should a website owner's maintenance of a website start to resemble an "online marketplace for illicit goods and services", then the website owner could potentially not receive protection under § 230.\textsuperscript{31} Under California law, Penal Code § 236.1 makes it a crime to traffic another individual.\textsuperscript{32} Present cyber and human trafficking laws do not appropriately address online human trafficking which is why there are several different proposals for dealing with this issue.

\textit{D. Potential Future Online Human Trafficking Regulations}

One of the most recent and potential pieces of legislation that is currently in debate in Congress is the Stop Enabling Sex Traffickers Act (SESTA). On August 1, 2017 SESTA was introduced to the Senate by Senator Rob Portman [R-OH].\textsuperscript{33} On September 19, 2017 SESTA was sent to the Committee on Commerce, Science, and


\textsuperscript{31} United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (demonstrating that an individual merely helps a willing buyer of drugs find a willing seller, and is therefore acting as a mere "steerer," is, without more, insufficient to establish a conspiratorial agreement; however, when a defendant steers buyer to sellers as part of a continuing business arrangement, or is otherwise the conduit for the transaction, criminal liability may attach). Though website owners may alter users' metadata information on advertisements without having crossed the line of being liable as a steerer or coconspirator, yet \"[c]laims that website facilitates illegal conduct through its posting rules necessarily treat website as publisher or speaker of content provided by third parties, and thus are precluded by Communications Decency Act (CDA).\" Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), cert. denied, 137 S. Ct. 622, 196 L. Ed. 2d 579 (2017).

\textsuperscript{32} CAL. PENAL CODE § 236.1 (2017).

\textsuperscript{33} Stop Enabling Sex Trafficking Act, S.1693, 115th Cong. (2017).
The purpose of SESTA is to amend the CDA in order to clarify that the CDA was never meant to protect providers and users of interactive computer services from Federal and State criminal and civil law relating to sex trafficking. In order to do this, SESTA would allow the providers and users of interactive computer services, website owners, to be liable for privately blocking or screening offensive material, and amend the “federal criminal code to specify that the violation for benefiting from ‘participation in a venture’ engaged in sex trafficking of children, or by force, fraud, or coercion, includes knowing conduct by any person or entity by any means that assists, supports, or facilitates the violation.”

In essence, website owners will be liable for the content of their users.

A second suggestion by other scholars desiring to address human trafficking crimes on the internet suggests that the CDA should include a “mens rea” requirement in order to protect innocent website owners from liability. In practice, this means that the requisite intent necessary to commit a crime, also known as mens rea, may be satisfied when website owners receive posts from their users or third parties and personally filter their websites of illicit content; furthermore, this would be the fulfillment of a mens rea because the website owner would have had a “state of mind of actually seeing these posts.” When this content is published by the website owner or the user after revision orders from the website owner, then the requisite actus reus, the act necessary to commit a crime, would be complete and both the website owner and the user of the website—the human trafficker—would be liable.

Moreover, a third hypothesis from different scholars would go so far as to advocate that non-regulation of the internet is a potential solution to regulate the internet because the internet is still developing and needs to evolve before “hast[y] interven[tion].”

---

34 Id.
35 Id.
36 Id.
37 Asención, supra note 5, at 261.
38 Id.
39 Id.
When the growth of the internet has slowed and “the effects of Internet use are plain, only then can the law hope to create a proper regulatory regime.”

All three of these potential ideas to combat human trafficking through regulation or non-regulation of the internet are further discussed later in this article. However, in order to address these three different proposals effectively, it is necessary to understand generally the vast context of the internet with a quick overview of the different tiers of the internet in order to have a better understanding of internet regulation.

E. The Three Tiers of the Internet

Lawmakers and the general public do not typically understand that there are different tiers of the internet, so in order to better understand how to regulate the internet, it is necessary to understand what tier of internet regulation is sought. The internet can be broken into three tiers: Surface, Deep, and Dark. The internet can be thought of as an iceberg. First, the Surface Web is the part of the internet that is accessible by standard search engines through indexing or Internet Protocol (IP) addresses. In iceberg terms, the Surface Web is the tip of the iceberg—what is seen above the waters. This part of the internet is what people are familiar with and understand to be the internet. However, below the tip of the iceberg is generally where the majority of its volume is located; likewise the Surface Web is not the majority of the volume of the internet. Second, the Deep Web is content hidden behind HTML forms and is beyond the reach of the typical user of the Surface Web. The Deep Web cannot be accessed by a majority of Surface Web users because it is typically business intelligence information that is only available

---

41 Id.
43 Id.
44 Id.
45 Id.
46 Id.
to those involved in the business such as a Gmail account.\footnote{Id.} The Deep Web represents nearly 550 billion documents, but some researchers say that the size of the Deep Web is infinite.\footnote{Id.} However, the Deep Web has been characterized as 90\% of the internet.\footnote{Andy Greenberg, \textit{Hacker Lexicon: What is the Dark Web?}, \textit{Wired} (Nov. 9, 2014), \url{https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/}.} In iceberg terms, the Deep Web is the part of the iceberg that is under the water and not seen on the surface of the water but is the majority of the iceberg’s volume.

The Dark Web is the hidden part of the Deep Web.\footnote{Brownlee, \textit{supra} note 42.} What is unique about the Dark Web is that it is a part of the web that comprises of special anonymity software Tor (The Onion Router), which encrypts user identity by bundling incoming data into encrypted packets, anonymizing information about the sender by stripping away part of its packet header, encrypting the remainder of the address information, and sending the encrypted data packet through several servers, called relays, en route to its final destination. In effect, this prevents others from identifying the user’s origin with its destination.\footnote{Sophia Dastagir Vogt, \textit{The Digital Underworld: Combating Crime in the dark web in the Modern Era}, 15 SANTA CLARA J. INT’L L. 104, 109 (2017). Tools and services are necessary to enter into the cyber-area known as the Dark Web. Therefore, at times this article refers to the ability for a user to hide, conceal their online identity, change their IP address, and alike as either Dark Web or Dark Web services.}

These networks, used to operate what would be considered as the Dark Web, make it “extremely difficult” to de-anonymize the users.\footnote{L. M. Brownlee, § 7A:8. \textit{Dark Web—Terminology}, Westlaw (database updated Apr. 2017).} Tor and I2P use systems to encrypt web traffic in layers and bounce it through “randomly-chosen computers around the world, each of which removes a single layer of encryption before passing the data to its next hop in the network” and in theory prevents users from
matching the traffic’s origin with its destination. The Dark Web is the part of the Deep Web that is intentionally hidden so as to be used for criminal purposes. Based on the nature of Tor’s design, “it is clear that dark web users subjectively believe their activity will remain anonymous, as that is the purpose of the dark web.” In iceberg terms, the Dark Web is the part of the iceberg that is nearly invisible on the surface and causes ships to sink upon collision with the iceberg.

**F. Effectiveness of Current Investigation and Prosecution of Human Trafficking**

Following the three tiers of the internet, it is now appropriate to analyze how effective current law enforcement is in dealing with trafficking. The Polaris Project, conducted by the National Human Trafficking Resource Center, researched human trafficking in America and found that the internet is the second highest venue for sex trafficking. Additionally, in 2014 alone, out of 24,062 signals that indicated potential human trafficking in general, 1,482 of these signals were from web forums and 1,149 were from emails. Also, out of 5,042 actual cases of human trafficking, 71% of those cases were specifically sex trafficking, and 4% were sex and labor trafficking. In addition, from December 7, 2007 to December 31, 2014 web forums and emails were 11.5% of the total human trafficking signals which indicated a potential human trafficking case. Although these are numbers, it is important to remember that the lives of real people are affected by the representation of these numbers.

---

53 Greenberg, *supra* note 49.
54 *Id.*
57 *Id.*
58 *Id.*
59 *Id.*
In 2013, on average 23.25% of sex traffickers were identified from the internet.\textsuperscript{60} For human trafficking in general, out of 379 cases, on average, 71.5% of the traffickers were not charged with a violation of the state’s human trafficking statute or any state criminal law.\textsuperscript{61} On the federal level, out of the 379 cases, on average 49.25% of the cases considered human trafficking were not charged with a federal trafficking statute or any other federal criminal statute.\textsuperscript{62} On average, for the states, 39% of the cases considered human trafficking instances actually charged the trafficker with human trafficking, 106 cases prosecuted the trafficker with compelling prostitution, and on average 20.25% of traffickers were charged with some other state offense.\textsuperscript{63} On average, out of 189 cases where the trafficker was charged, the more frequent crimes the trafficker was charged with on average was 27.5% harboring, 17.75% transport with the purposes of prostitution, or 13% other.\textsuperscript{64}

All states now have laws making human trafficking illegal; however, “few human trafficking cases were prosecuted under state human trafficking laws.”\textsuperscript{65} One of the main reasons investigators and prosecutors are not charging traffickers is that human trafficking laws are not necessarily laws that an investigator or a prosecutor would deal with on a regular basis.\textsuperscript{66} One prosecutor went so far as to say that the human trafficking laws are just for publicity stunts and are not practical because there are already other charges for the criminal that relate to sex and human trafficking such as kidnapping and sexual assault.\textsuperscript{67} This shows there is a lack of specialization in identifying the importance and implementation of human trafficking laws in institutions and communities.\textsuperscript{68} There are jurisdictions which are open to the idea of prosecuting human traffickers with the state trafficking statute, yet these institutions do not have the resources to

\textsuperscript{60} Farrell, \textit{supra} note 3, at 148.

\textsuperscript{61} \textit{Id.} at 151.

\textsuperscript{62} \textit{Id.}

\textsuperscript{63} \textit{Id.}

\textsuperscript{64} \textit{Id.}

\textsuperscript{65} \textit{Id.}

\textsuperscript{66} \textit{Id.} at 152.

\textsuperscript{67} \textit{Id.}

\textsuperscript{68} \textit{Id.} at 154.
implement specialized units or personnel who specialize in trafficking that are necessary to collaborate with law enforcement to proactively build a human trafficking case.\textsuperscript{69} Instead, prosecutors in these jurisdictions wait for the police to bring cases to them and then make the human trafficking connection themselves.\textsuperscript{70}

III. ISSUES WITH SESTA AND SIMILAR LAWS

As previously discussed, it is important to understand how the internet works and whether current human trafficking statutes are efficient. Now, considerations as to the effectiveness of SESTA and similar laws, a mens rea requirement proposal, and a nongovernmental regulation suggestion is up for discussion.

A. Prosecutoral Preference to Ignore Human Trafficking Laws

The data concerning the effectiveness of investigating and prosecuting human trafficking cases shows that human trafficking is still a new and developing concept for jurisdictions and institutions to grasp.\textsuperscript{71} Therefore, if general anti-human trafficking systems are hard to implement in these communities, then cyber human trafficking cases are going to be an even more difficult concept to urge jurisdictions and institutions to implement because it requires both cyber specialization and human trafficking knowledge for investigators and prosecutors. If prosecutors overlook human trafficking statutes because they are unfamiliar with this area of law, then prosecutors are likely to pass over cyber human trafficking statutes. For this reason, laws like SESTA, which would allow website owners to be liable for a users' content, are not the answer to cyber human trafficking. If investigators and prosecutors are hesitant in implementing internet statutes and human trafficking laws now, then prosecutors and investigators are likely to overlook more legislation in these areas. Also, they are likely to revert back to a preference to charge traffickers with laws they are more familiar with instead of online human trafficking laws.

\textsuperscript{69} Id. at 155.
\textsuperscript{70} Id.
\textsuperscript{71} Id.
Another issue with a SESTA-like law is that it mainly still focuses on the Surface Web and not the threat of the Dark Web. In the Surface Web, website owners are more easily identifiable; however, Dark Web website owners are not so easily identifiable because the servers, which comprise the Dark Web, conceal the identity of website users and owners. Therefore, SESTA-like laws are trying to deal with human trafficking on the Surface Web where it is easier to monitor website owners because they are identifiable. Yet, cyber human trafficking violations are still problematic in the Dark Web because it is hard to identify users and website owners. This means the website owners in the Dark Web do not screen the content of the website’s users because there is no way to identify the user from the website owners’ perspective. Further, investigators and prosecutors cannot easily identify a website owner and user. In the past, methods to combat online human trafficking have been wrongly directed towards the Surface Web. It is the Dark Web that needs to be regulated.

**B. Why SESTA and Similar Laws Have Negative Consequences**

In fact, SESTA-like laws have a negative effect in that if website owners (such as Google, Facebook, or Craigslist) are going to be held accountable for their users’ content, then website owners are going to heavily screen their users’ content before publication, which is the ultimate goal of SESTA – to keep website owners accountable for what is published on their site and to classify the website owner as a participant of sex trafficking. This means that cybersex traffickers will discontinue the use of these Surface Web websites to advertise out of fear of identification and capture. Therefore, in order to keep their anonymity, cybersex traffickers will go deeper into the web to not be found and conduct more of their activities in the Dark Web to avoid identification and capture. Thus, it will be more difficult to

---

72 See supra Section II(E).
73 Asención, supra note 5.
74 Id.
75 Vogt, supra note 51, at 109.
76 See infra note 88. San José Univ. Dep’t of Econ., supra note 10. Throughout this article, the actions of criminals and traffickers are hypothesized by a cost benefit analysis in order to understand potential outcomes of policy which can help
find human traffickers online who would normally risk advertising on the Surface Web because the risk would be too great now since both website owners and investigators will be looking to identify them.\textsuperscript{77} This means that fewer cyber human traffickers will advertise on the Surface Web, leading to fewer being caught and prosecuted. Statistically, this may look like a decrease in cybersex trafficking due to a fewer number identified and prosecuted individuals. However, the reality is that these criminal operations are now in the Dark Web.

Therefore, instead of jurisdictions and governments using time, money, resources, and manpower to find cybersex traffickers on the Surface Web, these communities and institutions need to spend more money to further specialize their investigators and prosecutors to find and prosecute online human traffickers who have gone into hiding from the Surface Web to the Dark Web. Instead of attacking the problem of human trafficking from the Surface Web and having criminals trickle down into the Dark Web, it is necessary to limit access to the Dark Web or to implement harsher punishment for criminals who operate in the Dark Web, as a method of deterrence from use of the Dark Web. This creates a situation where operating in the Dark Web is high risk, which would incentivize criminals to operate more in the Surface Web and Deep Web where they are more easily identifiable.\textsuperscript{78}

These approaches make cyber human traffickers easier to identify and prosecute, disable traffickers from hiding in the dark web, and disrupt their sex trafficking network and the network’s actors, which is a huge part of combatting cybersex trafficking.\textsuperscript{79} Public policy and constitutional concerns regarding freedom of speech, commerce, and privacy will be addressed, but it is important to note that because of the nature of the Dark Web services and servers that make it harder to identify its users, “any privacy expectation online is essentially

\textsuperscript{77} San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).

\textsuperscript{78} Id.

nonexistent, especially where the Internet is being used to further criminal activity.”

IV. ADDRESSING THE OTHER TWO INTERNET REGULATION PROPOSALS

As mentioned earlier, SESTA is one of three different proposals on internet regulation. SESTA was shown inefficient above, and this section addresses both the second proposal, that the CDA should include an intent requirement which in theory can protect innocent website owners from liability, and the third proposal, that nongovernmental regulation of the internet is the appropriate method to regulate the internet.

A. The Mens Rea Proposal is an Inadequate Internet Regulatory Scheme

For general criminal law, to obtain a successful conviction, a prosecutor needs to show that a suspect possessed an intent for the crime and took steps to accomplish the crime.\(^{81}\) It follows that if a mens rea\(^{82}\) requirement is necessary to prosecute criminals, then an intent element should be necessary to prosecute website owners who are not innocent but actually contributing to human trafficking.\(^{83}\) Like SESTA and similar laws, the problem with an intent element to prosecute website owners without violating § 230 of the CDA is that this requirement still only deals with the Surface Web and not the larger issue of human trafficking arising from the Dark Web. Though there are websites in the Dark Web, it is difficult to identify the website owner to show that the owner had the necessary intent requirement.\(^{84}\) The problem with anonymity in the Dark Web is still prevalent through this proposed method.\(^{85}\) Therefore, the intent

---

\(^{80}\) Vogt, supra note 51, at 118.

\(^{81}\) Mens Rea, Black's Law Dictionary (10th ed. 2014).

\(^{82}\) Id.

\(^{83}\) Asención, supra note 5, at 257.

\(^{84}\) Id. at 227, 237.

\(^{85}\) A mens rea requirement cannot be easily enforced on website owners in the Dark Web because of the anonymity that exists in the Dark Web, which prevents investigators and prosecutors from identifying website owners. Asención, supra
requirement would be difficult to implement because it would only be effective in the Surface Web not the majority of the internet and would not deal with the problems from the Dark Web.

B. The Nonregulatory Proposal is an Inadequate Internet Regulatory Scheme

Scholars who suggest nonregulation of the internet argue that “[w]hen the technology, when the experience, when the life in cyberspace presses us, only then should we expect law to understand enough to resolve these questions rightly.”86 They wish the internet will develop more so people can understand it better.87 One problem with this view is that the internet has been around since 1990.88 Thirty years is enough time to watch the internet grow and develop, and now is the time to regulate the internet. To wait any longer means lawmakers are going to need to play catch-up in their understanding of the internet’s development. Further, human trafficking would continue to ruin peoples’ lives. The injustices in the internet cannot continue into the future for the sake of the internet’s development. Rules of law and justice eventually domesticated the Wild West of America, and now it is time for internet regulation.89

note 5. Therefore, this mens rea requirement proposal would not address human trafficking as a deeper concern in the Dark Web and may only be effective on the Surface Web. This would then incentivize criminals to go deeper into the web to avoid government identification or Surface Web website owners. San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). Ultimately, the issue of a mens rea requirement proposal falls short similarly like the SESTA and similar laws proposal because they do not address human trafficking in the Dark Web and can actually incentivize criminals to do their activity in the Dark Web and not the Surface Web, thereby not really addressing the issue of human trafficking.

87 Id.
89 Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008) (stating that the “Communications Decency Act was not meant to create a lawless no-man’s-land on the Internet.”).
Another problem with nonregulation is that there are people who have the skills and tools to hack and maneuver the internet through methods unavailable to the general public.\textsuperscript{90} Elite groups of hackers are able to hack an organization's security system to reveal private information from and about the organization to the public.\textsuperscript{91} At times, these groups act as vigilantes. For example, the website Ashley Madison enabled its users to have affairs; and in response, a hacker group named the Impact Team hacked the "account information belonging to millions of users of the adultery website AshleyMadison.com, including some 15,000 email addresses possibly linked to government and military email addresses."\textsuperscript{92} Vigilante justice is not true justice because hackers pick and choose which organizations to promote or destroy based on personal bias.\textsuperscript{93} Therefore, the power is not with the people, but with those who have the best hacking tools and knowledge. True justice is not biased. The internet cannot regulate itself through nonregulation because those with tools and knowledge outweigh the voice of the general public.

Now that all three different proposals have been discussed and proven ineffective, it is necessary to discuss novel proposals.

V. PROPOSED LAW TO REGULATE THE DARK WEB

Ockham's Razor argues that the simplest answer to a problem is most likely the right one.\textsuperscript{94} A simple solution to combatting and dealing with human trafficking and other crimes in the Dark Web is


\textsuperscript{91} Id.


\textsuperscript{93} These internet vigilantes are not accountable to the people because the people cannot do anything to harm them since the general public does not have the type of knowledge and experience as other hacking groups. Governmental police powers are legitimate because people hold the government accountable through elections, protests, etc. Therefore, internet vigilante justice is not justice because they are not held accountable to the rest of the general public.

regulation. Proposed regulations discussed in the next section span from an implementation of government-mandated restrictions to disable anyone to use TOR and any type of cyber technology necessary for the Dark Web's existence, to an introduction of more stringent sentences for those who are successfully prosecuted for crimes they committed in or by use of the Dark Web.

A. Types of Dark Web Restrictions

The internet, though external and seemingly infinite, can be restricted. There are two methods of internet regulation. The first is hard censorship which requires the government or compelling intermediaries to exercise direct control over the internet infrastructure through law. The second is soft censorship which involves implementing laws to block material, paying for filtered access, or persuading intermediaries to restrict content. The idea of censoring and regulating the internet at first glance seems contrary to freedom of speech in the First Amendment; however, careful analysis proves that Dark Web regulation is legal and justifiable and keeps the Surface Web open to the public. Hard regulation of the Dark Web would disable access to services like Tor, which enable criminals to conceal their identity.

How can a country that values freedom of press, speech, association, and market reconcile with regulating the former when on the internet? Hard regulating and disabling access to Tor, other services like Tor, and other methods to gain access to the Dark Web, would allow the Surface Web to continue to be the uninhibited exchange of ideas and money. The problem with a completely free cyberspace is that the internet is insecure by aspirations to facilitate the most efficient exchange of information possible and a spectrum

96 Id.
98 Id.
100 Id.
of actors who exploit those insecurities.\footnote{101} Criminals exploit their anonymity on Tor and similar servers in the dark web which makes it difficult for investigators to track them because “data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it’s going.\footnote{102} Technology is evolving differently than any other human advancement. Tor makes it hard for investigators to catch criminals because Tor scrambles the Internet Protocol (IP) address.\footnote{103} Thus, technology has become an aider and abettor to criminals in the Dark Web since technology conceals the identities of criminals.

However, criminals can be found on the Surface Web because the server does not scramble IP addresses, which is a similar concept to

\begin{flushright}
\footnote{102}{TOR Project, supra note 97.}
\footnote{103}{Id. Here is how Tor describes itself:}
\end{flushright}

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tors users employ this network by connecting through a series of \textit{virtual tunnels rather than making a direct connection}, thus allowing both organizations and individuals to share information over public networks \textit{without compromising their privacy}. Along the same line, Tor is an effective censorship circumvention tool, \textit{allowing its users to reach otherwise blocked destinations or content}. Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features. \textit{Individuals use Tor to keep websites from tracking them} and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. \textit{Tor’s onion services let users publish web sites and other services without needing to reveal the location of the site}. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses. \textit{Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is, the more your anonymity will be protected}. \textit{Id. (Emphasis added)}

TOR’s sole purpose is to conceal an internet user’s identity. \textit{Id.}
an individual’s home address but for the internet. Thus, government services prohibiting anonymity in the Dark Web and servers that scramble IP addresses force criminals to trickle up to the Surface Web to advertise their activities. Because they are on the Surface Web, these criminals are easier to identify, arrest, and prosecute. As mentioned earlier, SESTA and similar laws focus on internet activity on the Surface Web which incentivizes criminals to leave the top tier of the internet where they are easily identifiable and move their activity to the Dark Web so they can have anonymity.

Whereas laws that make it illegal to start or use internet services that hide an individual’s internet identity would do four things: 1) force criminals who advertise in Dark Web networks and servers to the Surface Web where it is easier for investigators to identify and prosecute human traffickers; 2) force criminals who desire anonymity to search for such services in smaller networks which are easier to find and comb through than the massive amount of data in networks like Tor and other services in the dark web; 3) force criminals who do not want anonymity services because they would have to pay for them because of the associated risk, or because they no longer desire to advertise on the Surface Web or internet at all, to use traditional methods of advertising; or 4) discontinue their criminal activities because of new laws and risks. All four results are better than...
criminal in choosing how to act can be made from a cost-benefit analysis. It can be argued that though an activity is illegal, illegality in of itself does not eliminate the activity from existence. For example, murder is a crime, but murders still occur in this country. With this same logic, just because Tor and similar services would be illegal under this proposed method, that does not mean Tor and similar services are going to cease to exist. Though anonymity services on the web may still exist, there are still benefits to making such a service illegal.

First, large networks that provide anonymity would be illegal and forced to close shop by the government. This means that there are not huge networks with near limitless amounts of data in order to find criminal activity. What would happen is that criminal activity would either trickle up to the Surface Web or find smaller networks that would temporarily provide an anonymity service. San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). An argument has been made that lawmakers who seek to criminalize and deter sex trafficking on the internet are “woefully underprepared technologically to address the movement of this crime to more obscure corners of the Internet that are untraceable.” Dalton, supra note 108. Yet, it can be easier for investigators to find smaller networks that provide criminals anonymity on the internet rather than combing through massive amounts of data from larger networks to find the needle in the haystack. Therefore, it can be easier to find criminals who advertise illegal human trafficking exploits by causing Dark Web services of anonymity to be illegal because it will force the criminals to not be as anonymous by advertising on the Surface Web, which makes them easier to identify, or the traffickers will attempt to continue to be anonymous through illegal smaller networks which are still easier to find and comb through than a larger network. San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).

Second, investigators’ resources are better spent through this proposal because investigators will be able to find more criminals more easily when they advertise on the Surface Web due to the restrictions in the dark web and finding criminals in smaller illegal internet anonymity networks and providers would be easier. Therefore, investigators are not using resources, time, and money to try to comb through larger networks data for criminal activity and identify these criminals; rather they are actually finding the criminal activity quickly and identifying the traffickers.

Third, there will be a group of criminals who are not going to want to advertise on the Surface Web nor look to methods and networks to stay anonymous because of the price that will incur for such a service since it is illegal and there is a risk for providing the service, or the criminal just does not want to continue the activity through such a method. Id. Then, a criminal continues their exploits through traditional, old-fashioned methods which investigators and prosecutors already know how to combat.

Fourth, there will be criminals who are actually deterred from their human trafficking business because they do not want to find a way to continue to be anonymous on the internet, who will not want to advertise on any tier of the
allowing human traffickers while hiding under the cloak of the First Amendment, to advertise their illegal exploits anonymously. These four outcomes enable investigators and prosecutors to find criminal activity and human traffickers, do not abridge any First Amendment speech allowing for a free exchange of ideas to occur on the Surface Web where anyone can have access, do not change any laws affecting the Surface Web which can incentivize criminals to go to the Dark Web, and leave justice to the government as an unbiased party instead of to vigilante hackers with their own agenda.

Hard censorship of the Dark Web and deniability of users to Tor are extreme methods. However, a practical method of regulation can be done with similar results of deterring human traffickers from working in anonymity in the Dark Web. If hard censorship is controlled and shaped in the form of an applicable statute for prosecutors to apply on a case by case basis to criminals and deters criminals from their continued online human trafficking exploits, then legal access to the Dark Web and legal use of Tor is still protected. This concept is discussed in the next section.

B. More Stringent Sentencing for Criminals in the Dark Web

Under the current regime, traffickers are not deterred from posting commercial sex advertisements because they “are not afraid of who is on the other end of the information they submit.”109 These traffickers are either sending information to a potential client, in which case they benefit, or are communicating with government investigators, in which case these criminals do not fear because their identity is anonymous in the Dark Web with the use of TOR and other networks that allow a user to conceal their identity.110 Traffickers will continue to use the Dark Web unless they fear identification and the “exploitation value of each slave drops to a point where the risk outweighs pecuniary gain.”111 It is imperative to remember that human traffickers are in the business to make

internet, and who do not want to continue trafficking via the old-fashioned method. Id.

110 TOR PROJECT, supra note 97.
111 Dalton, supra note 108, at 1143.
money.\textsuperscript{112} They do a cost-benefit analysis where they analyze the benefit of their trafficking business in comparison to the associated costs and risks with trafficking and determine if the benefit is more worthwhile than the cost.\textsuperscript{113} Therefore, increasing the costs and risks for the traffickers changes their cost benefit analysis, and if the cost and risk is too high then traffickers then begin to fear who they send their advertisements and exploits to in the Dark Web.\textsuperscript{114} Thus, to incentivize traffickers to not continue their business via the Dark Web, the costs and risks of human trafficking must be greater than the benefit.\textsuperscript{115} One scholar calculated that a trafficked sex slave in the UK can bring a trafficker anywhere from \$156,000 to \$187,200 per slave.\textsuperscript{116} The real costs and risks are defined as maximum financial penalty in the law which is comprised of the probability of identification, probability of prosecution, and probability of conviction and sentencing.\textsuperscript{117}

In order to really increase the costs and risks in the human trafficker’s mindset, these probabilities and penalties must elevate to a level where the crime is minimally profitable or unprofitable.\textsuperscript{118} Governmental regulation of the Dark Web can increase the chances of identifying and prosecuting human traffickers.\textsuperscript{119} As for the probability of conviction and sentencing, the penalization of the crime needs to disinterest traffickers from continuing their business, because if the penalty is too low, then there is no teeth to the law.\textsuperscript{120}


\textsuperscript{113} San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).

\textsuperscript{114} Dalton, \textit{supra} note 108, at 1143; San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).

\textsuperscript{115} San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).

\textsuperscript{116} Dalton, \textit{supra} note 108, at 1143.

\textsuperscript{117} Kara, \textit{supra} note 112, at 140.

\textsuperscript{118} \textit{Id.}

\textsuperscript{119} See \textit{supra} Section V(C).

\textsuperscript{120} \textit{Id.}
In California, the punishment for violating Penal Code 236.1 includes a sentence of either 5, 8, or 12 years, and a fine of $500,000.121 Similarly, under 18 U.S.C.A. § Pt. I, Ch. 77 sections 1581 through 1597, the federal government generally sentences an offender to no more than twenty years coupled with fines.122 Though these numbers seem high at first, it is important to note that a majority of these cases are plea bargained for reduced sentences.123

Through plea bargaining, there is a real possibility that a zealous attorney for a wealthy trafficker could plea bargain for a sentence of three years with fines.124 Three years seems unjustifiable considering that the criminal may serve even less than three years because of good behavior while in prison. Furthermore, three years is unjustifiable because traffickers ruin people’s lives by forcing the government to spend time, money, and resources in order to decrypt a trafficker’s identity in the dark web. Moreover, three years is unjustifiable because the government continues to exert manhours and funds to prosecute individuals, taking up the court’s time. Therefore, a trafficker may not be frightened by the time spent in prison because plea bargaining might reduce the time of incarceration.

121 CAL. PENAL CODE § 236.1 (West 2017).
123 Sonya Tafoya, California’s Criminal Courts, PUB. POL’Y INST. OF CAL. (2015), http://www.ppic.org/publication/californias-criminal-courts/ (last visited Feb. 5, 2018). Where in 2013–2014, only 2% of criminal cases were settled by trial, 95% of Federal criminal cases ended in a plea bargain agreement. Lindsey Devers, Plea and Charge Bargaining Research Summary, BUREAU OF JUST. ASSISTANCE, https://www.bja.gov/Publications/PleaBargainingResearchSummary.pdf (Jan’y 24, 2011). Additionally, in most human trafficking cases where the prosecution needs to rely on an eye witness, the prosecution typically seeks a plea deal with the defendant because of witness unreliability, and, which was already discussed, prosecutors and investigators are unfamiliar and uncomfortable when applying the human trafficking statues. See supra Section II(F). Though a trafficking case can go through trial, the sentencing aspect does not require a judge or jury to implement the total confinement sentence. Standard 18.4.6 Judicial agency to perform the intermediate function, ABA STANDARD FOR CRIM. JUSTICE: SENTENCING (3d ed. 1994), https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice _section_archive/crimjust_standards_sentencing_blk/#6.4.
124 Three years is just a hypothetical number for the sake of the analysis and the flow of the reasoning for the argument.
for the human trafficker. Thus, to increase the costs to the trafficker’s costs benefit analysis, the prison time punishment for a human tracking violator must sufficiently deter criminal activity despite the trafficker’s own liberally calculated amount of years in prison and jail time through a plea-bargained deal.

Therefore, the sentencing guidelines for total time of confinement for human trafficking violations online needs to be increased. The American Bar Association (ABA) suggests that a legislative body should

create a sentencing structure that enables the agency performing the intermediate function to make reasonably accurate forecasts of the aggregate of sentencing decisions, including forecasts of the types of sanctions and severity of sentences imposed, so that the legislature can make informed changes in sentence patterns through amendment of the criminal code, or the agency can do so through revised guidance to sentencing courts.125

As shown in Section III of this article, jurisdictions and institutions are not taking advantage of charging traffickers with human trafficking statutes.126 For this reason, legislatures need to heed the suggestion of the ABA and amend the confinement time for a human trafficking violator according to what current prosecutors and investigators would deem effective. Currently, California and federal laws do not maximize the potential for the sentences to deter criminals from trafficking the innocent and do not incentivize prosecutors and investigators to utilize of human trafficking laws. Although human trafficking statutes already exist, there is another way to increase the time of confinement for an online human trafficker’s successful conviction: Prosecutors can charge an individual for improperly using the Dark Web.

126 See supra Section III(A).
C. Four Calculated Proposed Methods to Combat Online Human Trafficking

Human trafficking laws are already on the books and their time of confinements are already calculated. However, Dark Web regulations can be the solution to deterring a cyber trafficker. A human trafficker could be deterred if the prosecutor in that case charges them with the human trafficking statute and for a Dark Web statute because of the confinement times associated with a successful conviction of both charges. The following subsections discuss methods of regulating the Dark Web and how criminal statutes can successfully deter individuals from human trafficking crimes.

1. Calculating the Ideal Proposal to Appropriately Combat Online Human Trafficking

To effectively combat human trafficking in the dark web, two elements need to be appropriately considered: whether censorship by the government onto users of the Dark Web should be hard or soft, and the relationship of increasing the cost to the trafficker’s cost benefit analysis before committing the crime without overly increasing the government costs in pursuing the criminal.127 When comparing the relationship between these two elements for a new proposed law, there are four potential outcomes which Figure 1 demonstrates: 1) Governmental Total Ban in the Dark Web, 2) New Dark Web-Human Trafficking Statute Intertwined, 3) No Governmental Change, and 4) New Criminal Dark Web Statute that Attaches to Previously Existing Human Trafficking Statutes.

127 Brian Edgar Butler, Law and Economics, INTERNET OF ENCYCLOPEDIA OF PHIL., http://www.iep.utm.edu/law-econ/ (last visited Feb. 5, 2018). Ineffective laws and means of pursuing justice are those that increase costs of administration where another equally viable or better solution does not. Id. Therefore, a good new law would improve the legal atmosphere without over burdening it because overburdening courts, investigators, and prosecutors increases the cost of government. Id.
Each section within Figure 1 has inherent advantages and disadvantages. However, the “New Criminal Dark Web Statute That Attaches to Previously Existing Human Trafficking Statutes” (“Criminal Dark Web Statute”) is the best solution because there is no increase in costs to the government and the costs and risks for

---

128 There are two types of “cost” Figure 1 deals with: 1) Governmental Costs include money, resources, etc.; and 2) Costs to the Trafficker which is the cost of the cost-benefit analysis. San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). Where there is no governmental change there is no increase in either governmental or trafficker costs, all other sections of Figure 1 assume an increase in governmental and trafficker costs because the government in these instances is doing something more than it is now, an increase to government cost, to deter the trafficker, an increase to the Costs of the Trafficker. Id. However, with regard to “Hard Censorship,” the thought is the harder the censorship the increase of cost to the trafficker because this generally means more governmental regulation, oversight, or prosecution to the Dark Web which can increase the chances of the criminal’s capture. This means that the increase in governmental costs is not in relation to cost to the trafficker; rather, the harder the censorship is in proximity with an increase to the cost to the trafficker.

129 Though it is considered hard censorship, it is in and of itself is not technically hard censorship when tailored specifically to the human trafficking issue and no other crimes. However, in subsection 4 “New Criminal Dark Web Statute That Attaches to Previously Existing Human Trafficking Statutes” (“Attaching Criminal Dark Web Statute,”) it is discussed that this proposed Statute when
traffickers are increased. However, to properly show how the Criminal Dark Web Statute is the best solution, it is necessary to discuss and analyze all four methods.

2. Governmental Total Ban of the Dark Web (Total Ban)

A proposed set of statutes that would completely ban any kind of method to enter or create the Dark Web and anonymity in it would need to address the illegality of using or entering Dark Web services, the illegality of committing crimes by use of the Dark Web, and the illegality of creating or abetting Dark Web services as does the following proposed, hypothetical law drafted to demonstrate a Total Ban type of law:

(A)(1) Any network, server, provider, tool, or user that enables or aids an individual to conceal or change their IP address is illegal unless otherwise specified by law. (2) Any individual who intends to use and uses a network, server, provider, or tool that enables the individual to conceal or change his/her IP address in order to commit a crime shall be punished by doubling the total amount of possible time of incarceration for the original crime and doubling any and all fines associated with the crime.\(^\text{130}\) (3) Any individual with

\(^{130}\) As discussed above, the cost of human trafficking online needs to be greater than the benefits of the crime. San José Univ. Dep’t of Econ., \textit{supra} note 10. \textit{See supra} Section V(B). Therefore, for California, since the triad of potential incarceration time for violating the State’s human trafficking statute are five, eight, and twelve years in prison, with a large chance of any of these numbers plea-bargained, doubling the amount of the triads and starting the plea-bargaining process from the doubled amounts would be an appropriate deterrence to traffickers. \textit{CAL. PENAL CODE} § 236.1 (West 2017). Additionally, although the federal system lacks triads and the potential sentencing for a successful human trafficking conviction is no more than twenty years, a trafficker might still receive a
intent to violate Section (A)(1) and creates or aids a network, server, provider, or tool that enables a user of the internet to conceal their identity by changing the user’s IP address shall be punished by imprisonment for no less than seven years and fined no less than $500,000.\textsuperscript{131}

The benefit to this method is that it completely closes the Dark Web to not just human traffickers, but to all criminals and users of Tor and similar services. One issue with this proposal is it would require extreme government oversight to enforce, which would increase governmental costs. Under a law and economics approach, this proposal starts to become less effective because of the increasing costs of administration.\textsuperscript{132} Also, this type of proposed law is unlikely

\textsuperscript{131} The no less than seven years confinement and no less than $500,000 are arbitrary suggestions reasoning that any less time or fine would unsuccessfully deter violators of the law should the law not have any teeth as discussed before in Section V (B). San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). Therefore, doubling the maximum sentence to forty years for traffickers would deter crimes in the dark web. \textit{Id.} Ultimately, doubling the punishment is reasonable given the extra work prosecutors and investigators need to go through in order to identify the criminal online and capture the violator.

\textsuperscript{132} Butler, \textit{supra} note 127.
to pass since citizens' constitutional rights may be infringed, and Tor, and similar services enabling anonymity on the web, were created by the government. Therefore, this type of proposed method is not ideal to promote because of its lack of success to actually become law.

3. New Dark Web-Human Trafficking Intertwined Statute
(Intertwined Statute)

A law specifically addressing Dark Web Human Trafficking by intertwining Dark Web and human trafficking law is beneficial because it does not overwhelm prosecutors or investigators with the pressure of using a separate Dark Web statute. Here, the prosecutors can choose to either use the specific Intertwined Statute or the regular human trafficking statute.

On the federal level, the current law states the following: “Whoever holds or returns any person to a condition of peonage, or arrests any person with the intent of placing him in or returning him to a condition of peonage, shall be fined under this title or imprisoned not more than 20 years, or both.” An Intertwined Statute can state the following: Whoever holds or returns any person to a condition of peonage, or arrests any person with the intent of placing him in or returning him to a condition of peonage, shall be fined under this title or imprisoned not more than forty years, or both.

For California, the Human Trafficking Statute states the following:

236.1. (a) A person who deprives or violates the personal liberty of another with the intent to obtain forced labor or services, is guilty of human trafficking and shall be punished by imprisonment in the state prison for 5, 8, or 12 years and a fine of not more than five hundred thousand dollars ($500,000).

---

135 Id.
An Intertwined Statute can state the following:

236.1.5 (a) A person who deprives or violates the personal liberty of another with the intent to obtain forced labor or services, and who intends to and conceals or changes his/her IP address in order to violate this section is guilty of Dark Web human trafficking and shall be punished by imprisonment in the state prison for 10, 16, or 25 years and a fine of not more than one million dollars ($1,000,000).137

The reason both the proposed federal and California methods double the time of incarceration and fines is because this would double the cost to the human trafficker when calculating whether trafficking people is more profitable than the risk. This would ultimately deter the trafficker from the crime because of the increase to the cost while benefit remains the same.138

There are two potential drawbacks with these proposals. First, an Intertwined Statute is like trying to prove two crimes at once which can be confusing to prosecutors and jurors. Second, if successful, an Intertwined Statute can raise the cost of administration because prosecutors in other specialized fields would want a similar law for crimes they prosecute regularly. This would flood the legislature with proposals from investigators and prosecutors advocating a similar Dark Web statute for their field. The flooding of proposals and pressure to the legislature misuses the legislature’s time and thus costs governmental resources in both the advocates’ time and the legislature’s time debating the issue, which is all-in-all an ineffective use of the government’s resources and time.139 This proposed method is not ideal because a proactive law combatting online human trafficking ought not to vicariously overburden the legislature and increase the costs of administration through its success.

137 Id. (italicized text added to the existing statute).
138 See supra Section V(B).
139 Butler, supra note 127.
4. No Governmental Change (No Change)

There are reasons not to change how governments currently combat human trafficking. First, there would be no new cost to administration, legislation, investigation, and prosecution for states or federal governments that decide not to implement any change combatting cyber human trafficking. However, no change for the government means no change to the criminal behavior because no additional cost to the trafficker deters the criminal from trafficking.¹⁴⁰

Second, where the government decides not to change, prosecutors and investigators would be free to use the human trafficking statutes available to them at their whims. However, this means that prosecutors and investigators would continue not to be incentivized to use the available human trafficking statutes.¹⁴¹ This results in investigators and prosecutors not becoming more familiar and comfortable with convicting traffickers with the human trafficking statutes available. Juries and the public would not understand the dilemma of human trafficking and its negative effect on society. There would be no grander deterrence and cost to the trafficker to dissuade them from trafficking, and the problem of online human trafficking would still have no satisfactory solution.¹⁴²

Third, and finally, prosecutors could continue to focus on their specialty in the law. However, without change to the law there would be overlap in prosecution cases where trafficking prosecutors and cyber enforcement prosecutors must collaborate to successfully prosecute a trafficker operating online. The trafficking prosecutors would be able to prosecute the trafficker via the human trafficking statute but would need help from the cybercrime prosecutor to understand and prove what the trafficker did online is a violation of federal law to increase the potential detention time to a trafficker

---

¹⁴⁰ San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).
¹⁴¹ Farrell, supra note 3, at 152. See supra Section II(F).
¹⁴² San José Univ. Dep’t of Econ., supra note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis).
upon a successful conviction.\textsuperscript{143} As noted above\textsuperscript{144}, there are already federal and state laws that criminalize computer crimes.\textsuperscript{145} However, the state and federal laws have been charged in the past as vague.\textsuperscript{146} This presents problems for states and the federal government.

A No Change in the law presents more problems than solutions to combatting online human trafficking. On the federal level, the CFAA has been argued as too vague.\textsuperscript{147} This is one reason the two different prosecutors need to work together since cybercrime laws are too difficult to understand if a person has no specialization in that field.\textsuperscript{148} Though the Federal Courts have determined the CFAA not so vague as to consider the statute unconstitutional, the point is raised that the law is not entirely clear.\textsuperscript{149} For instance, section four of the CFAA states it is a crime to

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct further the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.\textsuperscript{150}

\textsuperscript{143} The same can be true where a cybercrime prosecutor would need the help from a trafficking prosecutor.

\textsuperscript{144} See supra Section II(A).


\textsuperscript{146} See generally the “Vagueness” section of 174 A.L.R. Fed. 101 (originally published in 2001); See generally the “Statute not unconstitutionally vague” section of California 87 A.L.R.6th 1 (Originally published in 2013).

\textsuperscript{147} See generally the “Vagueness” section of 174 A.L.R. Fed. 101 (originally published in 2001).

\textsuperscript{148} Two specialized prosecutors on one case is ineffective means of pursuing justice because the costs of administration go up while turnover is only for a single case. Butler, supra note 127.


\textsuperscript{150} 18 U.S.C. § 1030 (Westlaw 2008).
Here, the court decided that “simply bypassing an IP address, without more, would not constitute unauthorized use” of a computer, which is analogous to use of a computer that “exceeds authorized access.”\textsuperscript{151} This is important because changing or concealing one’s identity online via Tor or any other service that changes a user’s IP address could be viewed as a type of fraud. However, the court said that “bypassing” an IP address would not be a violation of the CFAA.\textsuperscript{152} Therefore, a person cannot be prosecuted through the CFAA because they altered their IP address in order to conceal their identity to commit a crime, specifically for this article the crime of online human trafficking.\textsuperscript{153}

Additionally, there are no other provisions of the CFAA that would criminalize the type of actions and behavior of traffickers who operate online when changing their IP addresses to stay anonymous in order to evade capture because the majority of the statute deals with defrauding the government.\textsuperscript{154} Therefore, on the federal level, there is no easy method by which cyber-crime prosecutors can prosecute online human traffickers. This presents two different problems. First, a human trafficker may not be convicted through cyber law but only just the human trafficking statute violation.\textsuperscript{155} Second, Government resources are used via the cybercrime prosecutor to creatively find a way to incorporate cyberlaw into the list of charges for the online human trafficker. Ultimately, two prosecutors are used for a single online human trafficking case which is not efficient costs of administration.\textsuperscript{156} Both of these difficulties show that no federal governmental change in this intersecting area of

\textsuperscript{151} Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016), \textit{cert. denied}, 138 S. Ct. 313, 199 L. Ed. 2d 206 (2017).

\textsuperscript{152} Id.

\textsuperscript{153} Id.

\textsuperscript{154} \textit{See generally} 18 U.S.C. § 1030 (Westlaw 2008).

\textsuperscript{155} This results in the human trafficker to receive only a sentence from the human trafficking violations. As mentioned earlier, these laws in and of themselves are not enough to deter the criminal from trafficking again because the cost is low relative to the profit. \textit{See supra} Section II(F). San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). Therefore, after serving the sentence the trafficker still has the same cost benefit analysis outlook that drives them to want to continue to traffic other human beings. Id.

\textsuperscript{156} Butler, \textit{supra} note 127.
law presents more problems than solutions to dealing with online human trafficking.

For California, Penal Code § 502, which is the California Computer Data Access and Fraud Act (CDAFA), is the controlling law for cybercrime in the State, and similar arguments made on the Federal level can be applicable to California.\textsuperscript{157} Similarly to the CFAA, the CDAFA has been charged as too vague, yet a district court held that the CDAFA is not unconstitutionally vague.\textsuperscript{158} Section four of the CDAFA states that a person can be charged when he or she

\begin{quote}
[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.\textsuperscript{159}
\end{quote}

Here, however, the legislature clearly intended the CDAFA to protect the public from criminals who wanted to interfere, damage, and unlawfully access computers, data, or computer systems.\textsuperscript{160} This means that the California Legislature’s intent was not to charge people for changing their IP address in order to conceal their identity online to evade capture for committing cybercrimes. Thus, prosecutors would not apply the law in such a fashion. Just like the CFAA, the CDAFA cannot be used to charge someone who changed their IP address to achieve a criminal gain, and there are no other sections, intended by the California legislature, of the CDAFA that can be used to charge someone who changed their IP address to conceal their identity to pursue their human trafficking endeavors.\textsuperscript{161} This means the two different problems analysis for the CFAA, in the

\textsuperscript{157} See first part of this section, specifically the two paragraphs before this State discussion.

\textsuperscript{158} See Oracle USA, Inc. v. Rimini Street, Inc., 2016 WL 3344377 (D. Nev. 2016). It is interesting to note that the CDAFA is more specific about terminology than the CFAA. The CDAFA defines basic terms like “data” which the CFAA does not. \textsc{Cal. Penal Code} § 502 (West2016); 18 U.S.C. § 1030 (Westlaw 2008).

\textsuperscript{159} \textsc{Cal. Penal Code} § 502(4) (Westlaw 2016).

\textsuperscript{160} Id.

\textsuperscript{161} \textsc{Cal. Penal Code} § 502 (West2016); 18 U.S.C. § 1030 (Westlaw 2008).
above paragraph, and CDAFA would be similar, meaning the CDAFA would have the same two problems as the CFAA.\textsuperscript{162}

Furthermore, the CFAA and CDAFA do not dissuade a criminal from trafficking a person because the cost of serving the prison time, in which the statutes indicate are not severe enough. On the federal level, an individual who violates section four of the CFAA can receive up to five years or a fine.\textsuperscript{163} For California, the crime is either a) a felony which is punishable by imprisonment for sixteen months, or two, or three years and a fine of $10,000 fine, or b) a misdemeanor punishable by imprisonment in a county jail for up to one year and a $5,000 fine.\textsuperscript{164} A maximum of five and three years may seem like a lot, but remember there is the possibility that a plea bargain may reduce these sentencings.\textsuperscript{165} Therefore, a human trafficker considering the costs/risks and benefits of trafficking an individual online may not think these specific years of prison as a deterrence when considering the plea bargaining years of incarceration.\textsuperscript{166}

At the end of the day there will be more problems than solutions if California and the Federal government do not change their procedures to deal with online human traffickers. Due to low sentencing guidelines, current federal and state laws do not effectively deter criminals.\textsuperscript{167} Moreover, a human trafficking prosecutor needs the assistance of a cyberlaw prosecutor because cyberlaws can be difficult due to vagueness and complexity.\textsuperscript{168} Two different specialized prosecutors working on one case is not an effective use of administration’s resources, therefore, this proposed

\textsuperscript{162} See first part of this Section (C4), specifically the two paragraphs before this State discussion.
\textsuperscript{164} \textsc{Cal. Penal Code} § 502 (West 2016).
\textsuperscript{165} \textit{See supra} Section V(B) above.
\textsuperscript{166} San José Univ. Dep’t of Econ., \textit{supra} note 10 (referencing specifically to show that the incentive for the criminal in choosing how to act can be made from a cost-benefit analysis). \textsc{Cal. Penal Code} § 502 (West 2016). 18 U.S.C. § 1030 (2008).
\textsuperscript{167} \textsc{Cal. Penal Code} § 502 (West 2016); 18 U.S.C. § 1030.
method is not ideal.\(^{169}\) A separate Dark Web specific statute that is easy to read and apply could be the remedy to the issues of the current laws’ drawbacks.

5. New Criminal Dark Web Statute that Attaches to Previously Existing Human Trafficking Statutes (An Attaching Criminal Dark Web Statute)

An anti-Dark Web statute would be a general statute applicable to all crimes and not just human trafficking. A criminal charge that attaches itself to other charges is analogous to California’s Gang Sentencing Enhancement Law.\(^{170}\) The gang statute states that a person who is convicted of a felony:

\[\text{[F] or the benefit of, at the direction of, or in association with any criminal street gang, with the specific intent to promote, further, or assist in any criminal conduct by gang members, shall, upon conviction of that felony, in addition and consecutive to the punishment prescribed for the felony or attempted felony of which he or she has been convicted, be punished as follows:}\]

\[(A) \text{ Except as provided in subparagraphs (B) and (C), the person shall be punished by an additional term of two, three, or four years at the court's discretion.}\]

\[(B) \text{ If the felony is a serious felony, as defined in subdivision (c) of Section 1192.7, the person shall be punished by an additional term of five years.}\]

\[(C) \text{ If the felony is a violent felony, as defined in subdivision (c) of Section 667.5, the person shall be punished by an additional term of 10 years.}\]\(^{171}\)

The prosecutor for a gang case needs to prove that the individual committed the crime, which upon a successful conviction, warrants a triad of possible time in prison, and then with this statute prove that

\(^{169}\) Butler, \textit{supra} note 127.

\(^{170}\) \textsc{Cal. Penal Code} § 186.22 (Westlaw 2018).

\(^{171}\) \textit{Id.}\]
the original crime was done for the benefit of the gang which then
punishes the individual for additional terms of incarceration.\footnote{Id.} Likewise, An Attaching Criminal Dark Web Statute would be proved
after the original crime, human trafficking. This would allow An
Attaching Criminal Dark Web Statute would add years of prison time
upon a successful conviction. Similarly, as in subsection one, “Total
Ban,” and subsection two, “Intertwined Statute,” doubling the
punishment significantly increases the costs to the trafficker in such a
way that would deter them from the crime.\footnote{See supra Section V(B).}

In the federal approach, when a prosecutor proves the elements of
human trafficking through the use of Dark Web, the sentence for
conviction would be no more than doubled twenty years and fines.\footnote{18 U.S.C. §§ 1581–1597 (Westlaw 2000).}
In California, when a prosecutor proves the elements of human
trafficking and that the defendant concealed their identity in the Dark
Web in order to commit a crime, the sentencing for the successful
conviction of the defendant would be to double the five, eight, or
twelve year time of confinement and the $500,000 fine.\footnote{CAL. PENAL CODE § 236.1 (West 2017).}
The benefit of a separate and general Dark Web statute, An Attaching
Criminal Dark Web Statute, is that this law can attach to other crimes
outside of human trafficking. Additionally, prosecutors are already
familiar with the concept of an attaching statute because of attaching
gang laws. Furthermore, prosecutors can choose whether or not to
use the statute, they would not be bound to use it but incentivized
through the doubled punishment. A doubled time of incarceration and
fines by An Attaching Criminal Dark Web Statute incentivizes
prosecutors to use the human trafficking statute which was not taken
advantage of before.\footnote{Farrell, supra note 3, at 152. See supra Section III(A).}
Lastly, An Attaching Criminal Dark Web Statute would be drafted in a way that it could be read, understood,
and applied easily by nonspecialized, cybercrime prosecutors and
jurors. These benefits, in addition to this proposed method not having
the drawbacks of the other three methods, is why An Attaching
Criminal Dark Web Statute is ideal.
6. An Attaching Criminal Dark Web Statute is Ideal Compared to the Other Three Proposals

As mentioned, prosecutors are incentivized to use An Attaching Criminal Dark Web Statute along with the human trafficking statute because of the stringent sentence which enables prosecutors and institutions to become more familiarized with human trafficking laws that were not taken advantage of beforehand.\textsuperscript{177} In addition, An Attaching Criminal Dark Web Statute is preferred to a Total Ban proposal because a Total Ban infringes on citizens’ constitutional rights, and would likely not be a reality since the government is one of the major players and founders of the Dark Web’s through Tor.\textsuperscript{178} In contrast, An Attaching Criminal Dark Web Statute allows legal use of the Dark Web, but only aims to punish those criminals who seek refuge in the Dark Web’s anonymity feature through a Tor or similar service. Therefore, An Attaching Criminal Dark Web Statute is constitutional and does not infringe on citizens’ constitutional rights, making it an ideal proposal for new legislation rather than a Total Ban.

Furthermore, An Attaching Criminal Dark Web Statute is favorable over an Intertwined Statute because of the Intertwined Statute’s two pitfalls. First, prosecutors and jurors can be confused with a statute that seems to require the prosecutor to prove two different crimes simultaneously.\textsuperscript{179} Second, an increase in costs of administration to the legislature by having to consider creating similar statutes for other prosecutorial fields by advocating investigators and prosecutors would lead to ineffectiveness.\textsuperscript{180} An Attaching Criminal Dark Web Statute would not confuse jurors and prosecutors because human trafficking and Dark Web violations would be two different statutes, which are easier for prosecutors and jurors to follow logically. Also, governmental ineffectiveness due to rising costs of administration by legislatures needing to hear and debate as to whether other prosecutorial fields should have a similar

\textsuperscript{177} Farrell, supra note 3, at 152. See supra Section II(F).
\textsuperscript{178} See supra Section V(C)(2).
\textsuperscript{179} See supra Section V(C)(3).
\textsuperscript{180} Id.
law would not occur with An Attaching Criminal Dark Web Statute because the statute has no limitations specifically to human trafficking online. Thus, An Attaching Criminal Dark Web Statute is ideal because it does not have the same drawbacks as an Intertwined Statute.

Lastly, An Attaching Criminal Dark Web Statute is more ideal to No Change to the government’s method of combating online human trafficking because the No Change method has numerous problems that An Attaching Criminal Dark Web Statute does not.

First, No Change adds no additional cost to the trafficker to deter them from trafficking, whereas An Attaching Criminal Dark Web Statute does add cost to the trafficker by doubling the punishment which dissuades the trafficker from continuing criminal practices.\footnote{See supra Section V(C)(4).} Second, No Change allows prosecutors to discontinue to use human trafficking statutes available; dissimilarly, An Attaching Criminal Dark Web Statute enables trafficking prosecutors to want to use both the Dark Web and human trafficking statutes because of the network they will destroy by keeping a trafficker in prison.\footnote{Id.} Third, No Change requires cybercrime prosecutors and human trafficking prosecutors to work on one case together which is ineffective use of government resources; while An Attaching Criminal Dark Web statute can be used by nonspecialized prosecutors and be easily understood by jurors.\footnote{Id.}

Fourth, No Change allows current cyberlaws to be vague, but An Attaching Criminal Dark Web Statute changes the status quo and allows for lawmakers to make more understandable laws.\footnote{Id.} Fifth, No Change allows current cyberlaws to continue to not criminalize concealing or changing an IP address to commit a crime or evade capture, while An Attaching Criminal Dark Web Statute does criminalize such activity.\footnote{Id.} Sixth, and finally, No Change allows the CFAA and CDAFA to continue not to deter criminals because of their low incarceration sentences; whereas An Attaching Criminal

\footnote{Id.}
Dark Web Statute does deter human traffickers because it would double the sentence of the original crime.\textsuperscript{186}

Therefore, An Attaching Criminal Dark Web Statute is more ideal than any other proposal because of its inherent benefits and it does not have any pitfalls as the other proposals. Though there are not any immediate policy concerns with An Attaching Criminal Dark Web Statute, there are some constitutional and jurisdictional issues that need analysis.

\textit{D. Potential Constitutional and Jurisdictional Issues with An Attaching Criminal Dark Web Statute}

A proposal that advocates for An Attaching Criminal Dark Web Statute necessitates the discussion of whether or not such a theoretical statute is constitutional and to decipher any jurisdictional issues. The constitutional issues that An Attaching Criminal Dark Web Statute seem to violate are the peoples’ rights of Freedom of Speech, Freedom of Commerce, and Freedom of Privacy, all primarily inherent in the First and Fourth Amendments.\textsuperscript{187} In order for An Attaching Criminal Dark Web Statute to be a viable proposal, it needs to be constitutionally sound.

1. First Amendment Concerns

The Right to Free Speech is the First Amendment to the Constitution found in the Bill of Rights.\textsuperscript{188} In addition, the Supreme Court has applied free speech to cyberspace.\textsuperscript{189} The courts desire to allow the internet to be a free space where people can be free and anonymous in sharing ideas like “political pamphleteering.”\textsuperscript{190} Does

\textsuperscript{186} \textit{Id.}

\textsuperscript{187} U.S. \textsc{Const.} amend. I and IV.

\textsuperscript{188} \textit{Id.}


that not mean An Attaching Criminal Dark Web Statute violates the First Amendment Freedom of Speech?

Additionally, the Supreme Court has said that a person’s First Amendment Freedom of Speech and Press protects a person’s right to be able to receive ideas and information no matter how obscene or its social worth.\textsuperscript{191} It can be argued that though states and the Federal Government have an interest in regulating commercial distribution of obscene material, they do not have an interest in controlling the right to receive information and ideas.\textsuperscript{192} In this day and age, internet commerce has flourished substantially from the commercial sex industry.\textsuperscript{193} Does this not mean An Attaching Criminal Dark Web Statute violates the First Amendment Freedom of Commerce?

Lastly, an individual has an inherent right to privacy found within the Fourth Amendment.\textsuperscript{194} The Supreme Court determined that a person is protected from governmental intrusion on his or her privacy if the person had a reasonable expectation of privacy.\textsuperscript{195} Does this not mean that An Attaching Criminal Dark Web Statute infringes on an individual’s right to privacy?

The simple answer to all three constitutional questions: no. It is important to focus in on what the First Amendment protects: legal speech, legal commerce, and legal privacy. Conspiracy is an example of illegal speech, selling cocaine is an example of illegal commerce, and being out in the open public is an example of when someone is not private. Therefore, it is possible that an act crosses the line from constitutional to criminal. Likewise, a person who enters the Dark Web atmosphere and conceals their identity by scrambling their IP address so as to avoid capture for advertising

\textsuperscript{192} United States v. Polizzi, 549 F. Supp. 2d 308, 383 (E.D.N.Y. 2008), vacated and remanded sub nom. United States v. Polouizzi, 564 F.3d 142 (2d Cir. 2009). \textit{See generally} Reno, 521 U.S. at 850–53. Additionally, some companies advertise that they will disguise or hide a client’s IP address and therefore an argument can be made that this proposal could affect this specific market, however see the rest of the subsection for clarification and answers. \textit{See ANONYMIZER}, https://www.anonymizer.com/ (last visited May 21, 2019).
\textsuperscript{193} Erin I. Kunze, \textit{Sex Trafficking Via the Internet: How International Agreements Address the Problem and Fail to Go Far Enough}, 10 J. HIGH TECH. L. 241 (2010).
people for sale is an example of where an act crosses into criminal liability and leaves constitutional legitimacy. A person does have a right to access the public sphere online in an anonymous manner; however, a criminal act is one that occurs when that anonymity is used to evade capture and prosecution under An Attaching Criminal Dark Web Statute perspective. Individuals are capable of participating in the free market online, but when that exchange is regarding the illegal sale of another human being then the sale becomes illegal and illegitimate. When a person goes into the Dark Web, a public area, they lose any expectation of privacy, especially when they wish to use such privacy to pursue criminal goals.\footnote{Vogt, supra note 51.}

Criminals should not be able to use the First Amendment’s Right to Free Speech, Commerce, and Privacy as a cloak for criminal activity online.\footnote{Asención, supra note 5.} Therefore, the time has come to regulate the use of the internet and have the government specifically outline when acts start to cross the line from constitutionality to criminality.\footnote{Importantly, An Attaching Criminal Dark Web Statute does not criminalize regular behavior and use of Tor and the Dark Web, but just using such services and opportunities for criminal activity which means the normal person is safe because it is very unlikely a normal citizen wonders onto a site or position of criminal activity. Reno v. ACLU, 521 U.S. 844, 854 (1997).}

2. Jurisdictional Concerns

There is a concern that should a legislature enact An Attaching Criminal Dark Web Statute that if they find out an offender is beyond their jurisdiction, and the other jurisdiction does not have a similar Statute, then what? For cyberlaw, some famous cybercrime “busts have occurred through international cooperation.”\footnote{Vogt, supra note 51.} Additionally, an argument was made that in order to combat a global culture based on the internet, jurisdictional laws and shared data needs to be more fluid.\footnote{Id.} Prosecutors and investigators desire to disrupt criminal networks, and this can be best be done by sharing evidence with other jurisdictions for the end goal of bringing criminals to justice.\footnote{Id. Farrell, supra note 3, at 152.}
As prosecutors and investigators from jurisdictions with An Attaching Criminal Dark Web Statute communicate and share their experiences of the statute, this can then inspire other jurisdictions to want to advocate to their lawmakers for a similar statute. Ultimately, if the end game is to end online human trafficking, then collaboration among borders is necessary and can help promote flexible laws to deal with an advancing technological world-culture.

VI. CONCLUSION

At the end of the day, online human trafficking is a contemporary scare for the public and lawmakers. Current internet and human trafficking laws fail to deal specifically with online human trafficking. SESTA and similar laws wish to deal only with the Surface Web and not the Dark Web, the area where cyber human traffickers tend to operate. Prosecutors and investigators do not currently take advantage of human trafficking statutes because of unfamiliarity and un-comfortability. Ultimately, SESTA and similar laws have a negative consequence of flushing online human traffickers from the Surface Web to the Dark Web in order to evade capture. A mens rea approach in regulating the internet to deal with cyber human trafficking is inadequate because it has similar negative consequences to SESTA and similar laws in dealing only with criminals on the Surface Web. A nonregulatory policy is also an inadequate solution since there is no real accountability to potential vigilantes.

There are two types of regulation schemes to the internet: hard or soft censorship. In order to incentivize prosecutors and investigators to use human trafficking statutes, while simultaneously increasing the cost of the “trade” to the human trafficker through increasing prison sentences upon a successful conviction, more stringent sentences are necessary for those human traffickers who operate in the dark web. In an analysis of the type of censorship and costs to the government, the four types of proposed methods to combat online human trafficking appropriately are Total Ban, Intertwined Statute, No Change, and An Attaching Criminal Dark Web Statute. The ideal proposed method is the Attaching Criminal Dark Web Statute because it does not have the same pitfalls as all the other proposals in addition to having unique
benefits.\textsuperscript{202} An easy to understand and apply Attaching Criminal Dark Web Statute is constitutional and potentially bridges jurisdictional concerns arising from technology and the current culture’s use of the internet.

The law needs to catch up to problems of current technology and issues of the internet. Legislatures need to deal with criminals in the dark web in a specific manner and not generally to the internet because the public and legislatures’ concerns are with those criminals operating anonymously online. Should lawmakers continue not to address the problem of criminals in the Dark Web, people’s lives will continue to be at risk. Anyone can be a victim to online human trafficking. It is time for lawmakers to specifically address this crime.

\textsuperscript{202} See supra Section II(F).