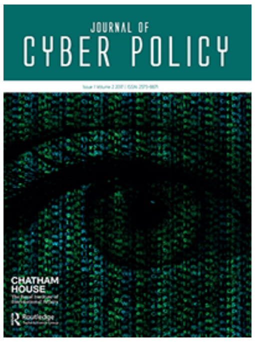

Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

A public policy perspective of the Dark Web

Michael Chertoff

To cite this article: Michael Chertoff (2017) A public policy perspective of the Dark Web, Journal of Cyber Policy, 2:1, 26-38, DOI: 10.1080/23738871.2017.1298643

To link to this article: https://doi.org/10.1080/23738871.2017.1298643

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 1, 26–38
http://dx.doi.org/10.1080/23738871.2017.1298643

Routledge
Taylor & Francis Group

A public policy perspective of the Dark Web

Michael Chertoff

The Chertoff Group, Washington, DC, USA

ABSTRACT
The Dark Web is at the centre of the debate over whether online anonymity should be maintained in spite of the illegal activity that it enables. Policy-makers must gain an understanding of the Dark Web in order to engage intelligently in the debate and enact effective Dark Web policy. This paper aims to provide context and policy recommendations pertaining to the Dark Web based on open-source research. The Dark Web's complete history, from its creation to the latest incidents of government intervention, remains relevant to today's debate. By examining cases where a government agency has enforced laws on the Dark Web, one can glean an understanding of which policies will be most successful going forward. This paper explores two specific policy topics: (1) determining the appropriate role of government in regulating the Dark Web and (2) exploring the most effective and reasonable methods for government to intervene. As the United States develops and refines policy regarding the Dark Web, the international community will also be manoeuvring to put in place regulations, and it is essential that these regulations be compatible while staying true to the values of the internet users that those governments serve.

ARTICLE HISTORY
Received 8 September 2016
Revised 20 February 2017
Accepted 20 February 2017

KEYWORDS
Dark Web; Dark Net; cybersecurity; anonymity; Deep Web; government; public policy; Tor

What is the Dark Web?

Introduction

Many consumers of the news have heard of the Dark Web. It is portrayed as a den of mysterious and illicit activity. Like most stereotypes, that is a misconception with some truth behind it. To shed light on the Dark Web, one must first understand what it is and how it differs from what most users wrongly consider to be the internet.

Actually, the internet comprises every single server, computer, and other device that is connected together in a network of networks. It can then be divided into two elements: the Surface Web and the Deep Web. The Surface Web is what the average user thinks of as 'the internet'. It is a collection of websites indexed by search engines like Google, Yahoo, and Bing that can be easily accessed through standard browsers and internet protocols. This may seem like a vast quantity of information, but the Surface Web is just the tip of the iceberg.

The Deep Web is the full body of the iceberg that remains mostly hidden from surface web users. Estimating the size of the Deep Web is challenging, but researchers estimate

CONTACT Michael Chertoff ✉ katy.montgomery@chertoffgroup.com

that it is between 4000 and 5000 times larger than the Surface Web (Finklea 2015). The Deep Web accounts for 90% of the traffic on the internet, which is a surprise to most users who do not realise they are accessing the Deep Web regularly (Greenberg 2014). Data from sites like Facebook, Twitter, or Snapchat are classified as the Deep Web because it can only be accessed through application program interfaces. Other large sections of data include instant messaging data and file-sharing services such as Dropbox and Google Drive (Greenberg 2014).

As this paper defines it, the Dark Web, by contrast, is a very small, hard-to-access portion of the Deep Web. It accounts for less than 0.01% of the sites on the internet: there are around 45,000 Dark Web sites and hundreds of millions of regular ones (Owen and Savage 2015). As explained below, the only way to access the Dark Web is by using a special browser like The Onion Router – Tor – and, often, a password. The Dark Web is generally anonymous, which makes it a sanctuary for cybercriminals and political dissidents alike. It has remained largely unregulated by the government, and the first step in better monitoring and policing the Dark Web is better understanding it.

The Dark Web or darknet is very often confused with the Deep Web, but the distinction between the two is very important. The Dark Web is a specific portion of the Deep Web and there are a few distinguishing characteristics that a site must meet to be considered a Dark website. The site must only be able to be accessed anonymously through a service such as Tor and cannot be accessed through the Surface Web. The site also must require a user to input its unique Tor address. Some Dark Web sites have an additional layer of security and may also require users to input a password. The reason most of the Deep Web is not considered part of the Dark Web is because it can be accessed through Surface Web applications.

The Dark Web has existed for a long time underneath the surface of the internet. The internet's development began in the 1960s as part of the U.S. Department of Defense's effort to network their computer systems, but the internet did not become a household name until the 1990s. The Dark Web itself remained obscure to most people, but it gained a measure of infamy in 2013, when Ross William Ulbricht (alias Dread Pirate Roberts), operator of the Silk Road, was arrested (Sui, Caverlee, and Rudesill 2015). The Silk Road was a marketplace for illegal goods and services accessed through Tor.

The Onion Router – an anonymous browser

Tor was originally developed for very different purposes. The Naval Research Laboratory (NRL) developed it at the turn of the twenty-first century with the aim of providing anonymity to U.S. military personnel engaged in operations abroad (Going Dark: The Internet Behind the Internet 2014). The system effectively makes it very difficult to determine the IP address that originally requested a site. To ensure the anonymity of military users, the NRL deployed it in October of 2003 as a free-to-the-public, open-source browser (Clemmitt 2016). This meant that military traffic was hidden anonymously in a crowd of anonymous civilian users.

The mechanics behind Tor's anonymity are actually fairly simple. The system works by sending a site request through at least three randomly chosen computers called relays (Greenberg 2014). Tor's name – 'The Onion Router' – actually comes from the fact that each computer adds a layer of encryption to the signal that only it can decrypt. The request then leaves a computer called the 'exit relay', which is the location from which the recipient perceives it to be originating (Finklea 2015). This makes users anonymous because exit relays might be making requests on behalf of hundreds of different users and randomising algorithms determine which exit relay is used. There are about 7000 volunteer computers worldwide that serve as relays (Clemmitt 2016). In effect, each request originator is hidden among the many layers of the onion.

Enabling mechanisms of the Dark Web – the Hidden Wiki and bitcoin

Tor was not the only development that enabled the creation and access of the Dark Web. There are two major services that serve practical purposes in enabling the Dark Web. Those are the Hidden Wiki and bitcoin. They each provide a solution that enables the Dark Web to be accessible and usable to those seeking it.

An early challenge for the Dark Web was that it was hard to find the hidden sites. The Hidden Wiki brought the first wave of users in 2004 (Darknet Markets Are Not beyond the Reach of Law 2016). This site contains a catalogue of all the Dark Web sites that are currently operating, user feedback on those sites, and information about what can be accessed through each site. Another way to find sites is by using Tor-specific search engines such as Ahmia, which indexes any hidden sites it can find, and Grams, which specifically finds hidden sites selling illicit drugs, guns, and counterfeit money (Finklea 2015).

In order to conduct actual transactions, Dark Web markets also began using a currency, bitcoin, which is pseudonymous and as difficult to trace as Tor. Bitcoin became the standard currency of the Dark Web. Bitcoins are an uninsured and variable currency that was created in 2009. They are stored in encrypted digital wallets. Bitcoins are designed to be very difficult to track back to the person who spent them. Each transaction is recorded in a public log, but only the wallet IDs are recorded, not the names of the buyer or seller (Yellin, Aratari and Pagliery, n.d.). In order to purchase bitcoins, a user must log into a bitcoin exchange, such as the popular Mt. Gox, where buyers and sellers trade traditional currencies for bitcoins (Yellin, Aratari, and Pagliery). Another way to get bitcoins is to mine them by donating a computer's processor time to solving complex math puzzles. While bitcoin is certainly the currency of today's Dark Web, Zerocoin is a currency in development which will be even more anonymous than current bitcoin transactions (Clemmitt 2016).

The Dark Web was developed in small steps, and it was not designed to be what it is today. Tor's creators at the NRL wanted a secure way for military personnel to communicate abroad. Hidden Wiki's founders created an index for average users to better understand and browse the Dark Web. Bitcoin was created to facilitate anonymous transactions. The creators of these technologies were privacy-minded, not ill-intentioned, but their intentions have not stopped illegal activity from blossoming in the shadows created by the Dark Web.

Benefits and drawbacks of the Dark Web's use

It is important to note that the vast majority of Tor's users are not necessarily accessing the Dark Web for illegal purposes. They may be using it to browse the Surface Web anonymously, often because they are located in a country that does not have free and open access to the internet. It may also just be because they are privacy-minded. There is another large contingent of Tor users who are performing Deep Web research (Sui, Caverlee, and Rudesill 2015). Finally, there are some Tor users who use the platform to access the Dark Web for criminal purposes.

Benefits

Tor's creators remain strong advocates of Tor's benefits. Roger Dingledine, an original developer, said, 'There are important uses for hidden services, such as when human rights activists use them to access Facebook or to blog anonymously,' and that 'These uses for hidden services are new and have great potential' (Ward 2014). Tor is a tool which can be used anonymously for both legal and criminal purposes. While it is essential to acknowledge the important role that anonymity plays in protecting human rights activists from oppressive regimes, it is also important to consider the challenges that anonymity poses to the law enforcement community.

Runa Sandvik, a security researcher who worked on Tor, explains that Tor was opened up to the public because

> if you have this anonymity system and [all] traffic going into the system is the U.S. Navy and everything popping out is the U.S. Navy, then you're not that anonymous … by opening up this system to everyone, different groups of people can hide in a big crowd of anonymous Tor users. (Going Dark: The Internet behind the Internet 2014)

She goes on to explain that Tor is helping nearly one million internet users seek out a truly free internet on a daily basis (Going Dark: The Internet behind the Internet 2014).

Tor was not the first service to offer anonymous browsing online. In the 1990s, Ian Clarke created Freenet, a peer-to-peer web browsing service. Today's internet actually resides on a few central servers that can be targeted and taken down or controlled by governments (e.g. the 'Great Firewall' of China). Freenet distributes data across the network so that it is stored in a decentralised way that protects information from being tampered with by hackers, government or otherwise (Stevens, n.d.). When asked about his motivation for creating Freenet, Clarke said, 'I believe in the concept of democracy […] I believe at a fundamental level, people's freedom to exchange information and ideas is fundamental to the legitimacy of democratic government' (Stevens, n.d.). Freenet differs from Tor in that Freenet is its own network, while Tor is an anonymous means of accessing the already-existing internet, but both were created in the name of protecting the freedom of the internet.

There are many legal uses of Tor. Many people use it to protect browsing privacy. For example, e-book collections of subversive works are available on the Dark Web, away from government censors. There are also sites set up specifically for journalists to share files and stories. These sites serve as an important pipeline that reporters can use to smuggle out important stories that portray authoritarian regimes in a negative light. Finally, there are secure image-sharing sites that offer ordinary citizens an additional layer of privacy when sharing sensitive photos (Sui, Caverlee, and Rudesill 2015). All these uses may be perfectly legal and understandable, but the reality remains that they only account for a portion of Dark Web traffic. Much of the traffic on the Dark Web is illegal.

Drawbacks

Indeed, most Tor users are just seeking privacy and may be using Tor for legitimate reasons. Only 1.5% of Tor users are actually accessing the Dark Web, although they generate a lot of traffic (Ward 2014). The trouble is that Tor and the Dark Web are virtually inseparable. It is impossible to make a tool that keeps users anonymous while also tracking their activity to make sure that they are not accessing illegal websites. Tor's creators would like to think that the browser mainly carries the traffic of journalists valiantly writing stories from countries without laws protecting free speech, but that is not the case. The majority of traffic to hidden Dark Web sites using Tor is for viewing and distributing images of child abuse and purchasing illegal drugs.

Child abuse accounts for the largest portion of Dark Web traffic. Dr Gareth Owen and Nick Savage, researchers at the University of Portsmouth, conducted a six-month study that explored Tor's usage and hidden services. They concluded that more than 80% of Tor traffic requests to hidden sites that were observed in the study were directed towards known child abuse sites (Owen and Savage 2015). They did acknowledge that this data may not be a perfectly accurate representation, since government agencies often use computers that will automatically access websites containing images of child abuse as a part of their investigation. It is virtually impossible to determine what portion of the 80% is police activity and what portion is traffic created by a human at a computer. Even if half of the child abuse traffic observed were police activity, much user traffic remains on the Dark Web targeting child abuse sites.

Indeed, child abuse images are not isolated to the Dark Web. A charitable foundation, called the Internet Watch Foundation, performed a study in 2014 as part of their work to minimise the distribution of images of child abuse. They found 31,266 internet URLs with images of child abuse on them, but only 51 (about 0.2%) were on the Dark Web. (It is worth noting here that the methods used to find sites on the Dark Web may not have found all the Dark Web sites that were available, and thus may be skewing the number to look like a lower-than-accurate percentage of websites containing images of child abuse that are on the Dark Web) (Clemmitt 2016). This statistic indicates that the Dark Web, while it enables cybercrime, is not the only way that cybercrime is enabled.

Drug traffic is the subject that is most commonly associated with the Dark Web, and it is an integral part of Dark Web marketplaces. In fact, it represents the largest percentage of Dark Web hidden sites in Dr Gareth Owen's study on Dark Web browsing habits (Owen and Savage 2015). These sites are actually easier for enforcement officers to infiltrate because the officers are capable of better hiding their identity when they go undercover. Additionally, the drugs do have to be physically delivered, which leaves a window open for traditional policing to apprehend the dealers.

One of the largest and most infamous Dark Web marketplaces was Silk Road. It was created in 2011 by Ross William Ulbricht who hid under the alias of Dread Pirate Roberts (DPR) (Finklea 2015). It is estimated that DPR received over $13 million in commissions from allowing vendors to use his Silk Road platform. In October of 2013, the FBI shut down Silk Road. As part of their investigation, they determined that over $1.2 billion in sales had occurred involving 150,000 customers and 4000 vendors (Sui, Caverlee, and Rudesill 2015). These staggering numbers show the scale of illegal trade on the Dark Web. Ulbricht was tried and sentenced to life in prison in May of 2015 (Finklea 2015).

The 2013 shutdown of Silk Road was not the end of Dark Web marketplaces. In fact, many more sprung up to take the place of Silk Road. These platforms do not just sell drugs. They sell anything that vendors want to put online. Just weeks after the 2013 credit card breach at Target, Dark Web markets were selling stolen credit cards at a rate of $20 to $100 per card (Finklea 2015). There is clear demand for a black market online, so it is not an issue that will dissipate on its own. Governments must work to enact policy that will address the challenges put forth by the Dark Web in a thoughtful and intentional matter.

Grey area

There are two specific areas of Dark Web activity that cannot reasonably be categorised as entirely beneficial, but have some admirable characteristics: whistleblowing and hacktivism. Whistleblowing is an essential part of what keeps democracies in check, but it can dangerously expose government methods and sources if it is not done through official channels. The Dark Web was used by whistle-blowers such as Chelsea Manning, Julian Assange, and Edward Snowden to expose government secrets (Sui, Caverlee, and Rudesill 2015). If these whistle-blowers had used legal, congressional channels to make their complaints, the matters could have been handled without publicly disseminating classified information.

Hacktivism is another issue that is not black and white. While the aims of some hacktivists may be debatable, their methods are often offensive, and more importantly, illegal. For example, in October of 2011, Anonymous, a hacktivist group, crashed a website hosting service called Freedom Hosting, using a Distributed Denial of Service (DDoS) attack. They did this by tracking the signatures of the child abuse websites that Freedom Hosting hosts back to the server. The hackers also stole the credentials of 1500 users of Lolita City, a child abuse website, and leaked them online (Finklea 2015). The aim of taking down a child abuse website is certainly honourable, but vigilante justice has no place on the internet as perpetrators cannot be held accountable for their actions.

Policy issues pertaining to the Dark Web

Creating policy to address the Dark Web requires an understanding of the benefits and risks of anonymity and of an open internet. Rash and sweeping legislation has the potential to encroach on civil liberties and to be a nightmare to enforce. On the other hand, not addressing the Dark Web will allow illicit activities to persist unabated. It is impossible to regulate the Dark Web in isolation; any regulations must be applicable to the internet as a whole and will thus affect Surface Web users, Deep Web researchers, and Dark Web criminals alike. This section will explore two important policy issues surrounding the Dark Web: the appropriate role of government, and the tactics that government enforcers should employ.

Major policy issue 1: What is the appropriate role for the government in the Dark Web?

When new technologies arise, the government must determine its role in regulating them. Technological progress can change the ways our laws apply and necessitate new laws. For example, the United States is still struggling to adapt old laws governing telephones and television to the internet. The Dark Web is a brand new topic to many policy-makers, and it is essential that they become informed before enacting policy rather than learning from mistakes. Current U.S. laws are vaguely applicable to the Dark Web, but government agencies have not solidified policies on how to regulate it within a legal framework.

The most important Dark Web policy issue is regulating Tor. The Dark Web could not exist without anonymising technology. Anonymity is the crux of what makes the Dark Web different from the Surface Web, so policy regarding anonymity and, by extension, the use of Tor, is most relevant. There are two central challenges to creating policy for the Dark Web: protecting anonymity and working internationally. Policies regarding the Dark Web must be clear and internationally agreeable, without compromising the ideals of the American people.

The first challenge is that there is nothing inherently criminal about using Tor for anonymity, but there is no clear way to sort the criminals from the innocent users if they are all anonymous. If there were no criminals using Tor, the law enforcement community would not be pushing so hard against the anonymity that it provides. Unfortunately, it is very difficult to hold someone accountable for their actions if their identity is unknown, and it is hard to unmask one person without having the capability to deanonymise everyone else using Tor.

The second challenge is that the internet is inherently very international, which makes coordinating regulations challenging. One country does not control the entire internet, and as much as some nations would like to have full control over the ideas coming in and out of their country, they have not fully achieved success with a 'great firewall'. The internet cannot be regulated country by country without destroying the benefits that the internet brings to all countries, so finding consensus is important. There is some content, such as images of child abuse, that all countries agree should be illegal and banned across all distribution outlets. There is other content however, like political dissidence, where different countries have dramatically different stances.

The United States currently has some laws that are applicable to Dark Web activity, but they were not specifically designed to meet the challenge of the Dark Web. For example, hacking is often enabled by the Dark Web. Hackers will purchase malware from other hackers, or will use a Dark Web method of collecting ransom from ransomware attacks. Hacking is regulated by the Computer Fraud and Abuse Act (CFAA), which bans trespassing on, unauthorised accessing of, and damaging computers in interstate or international commerce. The CFAA also bars trafficking, unauthorised computer access, and computer espionage (Sui, Caverlee, and Rudesill 2015). These U.S. regulations are perfectly sufficient to handle hacking, but they do not specifically tackle the challenge of anonymity online, and they are not necessarily effective beyond U.S. borders, from where most cybercrime against the U.S. is launched. Regulating cybercrime on the Dark Web therefore becomes exponentially more challenging when the international community is brought in.

Three members of the international community have each pushed agendas relating to Tor that are inconsistent with the aims of the U.S. government. China has made efforts to block access to Tor, Russia has made efforts to deanonymise Tor for political purposes, and Austria has made efforts to eliminate Tor traffic within its borders. U.S. regulators must be cognizant of the diverse sentiments of the international community. While countries such as the U.S. and Germany have supported Tor, going as far as to fund it, other countries are vehemently opposed to it (Tor: Sponsors, n.d.). This poses a major challenge to international policy development. China has some of the strictest and best-enforced policies regarding internet regulation. They heavily censor online conversation and quickly silence those who speak out for collective action or otherwise threaten the regime (King, Pan, and Roberts 2013). There are many free speech advocates in China, including Murong Xuecun, who strongly support the Dark Web because it empowers them to speak freely. Xuecun has warned that 'the great firewall' creates 'a Chinese information prison where ignorance fosters ideologies of hatred and aggression' (Clemmitt 2016). China certainly takes seriously the threat that Tor poses to their information control. In 2008, China blocked the Tor project's website in an effort to prevent users from downloading the service. Then in 2009, China sought to block all of the public relay computers that Tor employs to anonymise users (Clemmitt 2016). The Chinese government released the following statement regarding the internet in a 2010 white paper: 'Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty,' and Chinese 'laws and regulations clearly prohibit the spread of information that contains content subverting state power, undermining national unity [or] infringing upon national honour and interests' (Clemmitt 2016).

China is in the company of Russia, which recently passed some of the strictest and most oppressive laws regarding internet use and Dark Web activity. On 2 August 2016, Russia's Federal Security Service began enforcing the collection of encryption keys from internet service providers. A refusal to turn over keys can result in a one million rouble fine ($15,000) (Vitaris, Russian [Sic] is collecting encryption keys as 'anti-terrorism' legislation goes into effect, 2016). The Russian government has also made efforts to break the anonymity of the Dark Web. They entered into a contract with Rostec worth 3.9 million roubles (around $60,000) to 'research the possibility of obtaining technical information on users of [the] anonymous network Tor and users' equipment' (Vitaris, Russian Government Sues Firm for Failing to Deanonymize Tor Users 2015). Rostec was unable to hack into the Tor project by the due date of November 2015, and the Russian government is now suing them for the failure.

One of the most dramatic policy actions was taken by Austria in 2014. Authorities arrested a man who had made his computer a Tor relay, and held him accountable for 'contribut[ing] to the completion' of a cybercrime committed by another Tor user who had no involvement with the arrested man, beyond the fact that the cybercriminal's traffic was routed through the Austrian man's computer (Clemmitt 2016). The verdict has set a precedent that it is potentially illegal to operate a Tor exit relay in Austria, which is a major blow to Austrians who wish to support the project. Cooperation between Austria and the U.S. would be challenging given how strongly the Austrian government opposes the service and how this contradicts the U.S. legal precedent of not holding tools responsible for the actions of their users.

Like all battles, the battle between Tor and the governments that wish to shut it down is two-sided. In response to China's action of blocking all known IP addresses of Tor relays, Tor has created special relays called bridges. Their IP addresses are kept secret, and users must go through a lengthy application process to request the IP address of a bridge if they wish to access the network. This application process is no problem for Chinese Tor users who are willing to go to considerable lengths to connect to the network, but it poses a major challenge to the Chinese government's goal of blocking all the IPs, because they cannot just request them all at once, and as long as any one bridge is open, Chinese users can connect to Tor (Clemmitt 2016). This just goes to highlight the fact that access to the Dark Web is a dynamic challenge. Yesterday's policy may no longer be applicable today.

The United States must rise to the challenge of enacting policy that successfully strikes the balance between protecting user anonymity and preventing illegal activity online. Nations around the globe have different stances on how best to tackle the challenge of Tor. Given that international cooperation will be essential, governments must work together towards creating smart Dark Web policy. The specific tactics for intervening on the Dark Web must be carefully considered. Many governments, including the U.S. government, have made attempts in the past with varying degrees of success. By learning from past mistakes, leaders can create policy that effectively addresses the challenge of tomorrow's internet.

Major policy issue 2: What are the appropriate tactics for government intervention on the Dark Web?

Once the United States government has determined its role in regulating the Dark Web, it must decide which tactics it will use to carry out that role. The government must use tactics that take down criminal Dark Web activity while protecting the anonymity of innocent users to the maximum extent possible. In the interest of not compromising any confidential information, the tactics explored in this section are those that have been publicly released. This section will discuss the lessons that can be learned from previously used tactics. The most effective and reasonable tactics are those that can target specific anonymous users and hold them accountable for their actions rather than deanonymising vast swathes of user data.

The combined capabilities of a small handful of government agencies can be effectively employed towards the end of policing the Dark Web. The FBI has had the capability to use a computer and internet protocol address verifier (CIPAV) to 'identify suspects who are disguising their location using proxy servers or anonymity services, like Tor' since 2002 (Finklea 2015). This technology allows Tor traffic to be flagged separately from regular internet traffic. It does nothing to compromise the anonymity of users, but it is helpful in narrowing down search parameters when the FBI performs an investigation. The Department of Defense's Defense Advanced Research Projects Agency (DARPA) is developing a tool called Memex, which can uncover patterns to help law enforcement combat illegal activity (Finklea 2015). This project is another way that investigative agencies could make sense of Tor traffic without having to unmask all Tor users. Instead, investigators could detect specific patterns and then track down the specific user making the suspicious requests.

An important case study occurred in February of 2015. The FBI used a hacking tool to identify the IP addresses of users accessing a hidden Tor child abuse site called Playpen (Cox 2016). Within a month of being launched in 2014, Playpen had 60,000 member accounts. By 2015, there were 215,000 accounts, 117,000 posts, and 11,000 unique visitors per week (Cox 2016). In order to take down the site, the FBI took the unprecedented move of seizing the Playpen server and transferring the site to an FBI server, under a warrant issued by a federal magistrate judge in the Eastern District of Virginia (Satterfield 2016). The FBI ran Playpen off their server from 20th February to 4th March of 2015 and were able to access the computers of about 1000 Playpen users during that time. That resulted in sufficient evidence to bring about 1500 cases against people accessing images of child abuse on Playpen (Cox 2016). This tactic managed to capture only those who were accessing the child abuse site while leaving other users of Tor untouched. While some may have ethical qualms about the FBI running a child abuse server for a couple weeks, there is a strong argument to be made that by identifying the users, the FBI was able to prevent further access to images of child abuse in the future. As a result, Tor users will feel slightly less protected by their anonymity when they are accessing illegal sites, but other people who browse using Tor regularly can still enjoy comfort and anonymity in their legal activities.

Legal frameworks are essential in supporting criminal investigations. There is a debate over whether the federal magistrate judge from the Eastern District of Virginia had the legal authority to issue a warrant that led to searches outside the judge's district. This is an example of current U.S. laws not keeping up with evolving technology. The FBI maintains that the warrant was valid because the server was being run from a site located in the judge's district (Satterfield 2016). However, in the nine cases that have been brought so far using evidence from this sting operation, six judges have written opinions to indicate that the first federal judge did not have the authority to authorise searches outside his jurisdiction (Satterfield 2016). The problem that arises from this debate is that it would have been impossible to identify the users of Playpen, and then get warrants for each user, if it had not been for the tool that the FBI installed on the server. To be clear, the FBI later got individual warrants to search the computer of every suspect identified in the case (Satterfield 2016). A policy solution must be found which gives the FBI a stronger legal footing for employing such an effective investigative technique in the future.

The takedown of Silk Road was a case where FBI tactics were somewhat less than fully successful. To be sure, the operator, Ross Ulbricht, was arrested, but since the FBI shut down Silk Road in October of 2013, there has been an explosion in the darknet market for illegal goods. The market was previously centralised around Silk Road, but it has become more fragmented. There is a Reddit directory of Dark Web marketplaces that is updated to inform users which ones are reputable and which ones are unreliable, and the list of untrusted sites is far longer than the list of trusted ones (Swearingen 2014). Almost immediately after Silk Road was shut down, users flocked to a previously unknown site called the Sheep Marketplace. This site dominated the Dark Web market until a vendor exploited a vulnerability and stole $6 million in bitcoins (Swearingen 2014). Silk Road 2.0 was launched by former administrators of the original Silk Road on 6th November 2013. This came only one month after the original Silk Road was shut down. Silk Road 2.0 was short-lived. It was hacked in February 2014 by a vendor who stole $2.7 million in users' bitcoins (Swearingen 2014). That was not the end of the Silk Road however. Silk Road 3.0 is considered the most resilient Dark Net market and has been operational since May 2016 (Darknet Markets Are Not beyond the Reach of Law 2016). Thus, while the government took down the original Silk Road, it is clear that that operation was not entirely successful, as it did little to dissuade people from starting new Dark Web marketplaces, and it did not hold vendors or customers accountable for their transactions on the site. As Eric Jardine points out, these criminal activities conducted on the Dark Web may be knocked down, but other programmes emerge and simply take their place (Jardine 2015).

Another unsuccessful case of government intervention in Dark Web matters came in March of 2015 when federal investigators served a subpoena to Reddit in which they demanded the personal data of five users who accessed r/darknetmarkets, a forum where users discussed illegal online marketplaces (Finklea 2015). This was an unwise action because it discourages future discussion on open forums such as Reddit. If criminals are driven away from open and easy-to-monitor pages and towards pages that are hidden in the Dark Web, it makes the FBI's job of finding cybercriminals much more challenging.

The three case studies described above cover the spectrum from effective to ineffective enforcement. The best tactics are those that are narrowly focused, like the ones the FBI employed to take down Playpen. In other words, these tactics search for the criminals in places where anyone visiting the site is a criminal. This is the best of both worlds because it allows for long-term deterrence while protecting user privacy to the maximum extent reasonable. In the interest of continuing to be effective, the FBI must be given a stronger legal framework to perform such investigations. The tactic that was used with Silk Road, of merely taking down a site, has a short-term pay-off, but it is largely ineffective in the long run because other marketplaces will pop up to meet the demand. The tactic that was employed with the Reddit forum was essentially a failure. It did nothing to deter illegal activity, and it squandered an opportunity to monitor discussion in the open and more tactfully identify those involved with illegal activity. In examining these cases, it is clear that tactful, carefully directed operations will be most successful in deterring future illegal activity on the Dark Web while being mindful of innocent users' privacy.

Conclusion

The Dark Web is, by its nature, anonymous and incapable of discriminating between criminals and ordinary users. Enforcement agencies must address this issue by employing tactics that maintain the privacy of the average user while unmasking the criminal.

The most effective way of doing this is by looking for the illegal sites instead of the illegal users. Under proper legal authority, government hackers can place deanonymising tools onto the computers of users accessing the site. If the government merely shuts down the site, another will pop up in its place. On the other hand, if enforcers bring charges against the users of an illicit site, future users who are considering accessing illegal sites will be more hesitant to do so because of the risk of getting caught. The final option would be for the government to attempt to break Tor, in other words, to identify every Tor user. This, given the past trend with Silk Road, would likely result in a more robust version of the service being created, thwarting the government's efforts. It would also destroy a useful tool for legitimate users, like dissidents.

Understanding the best enforcement techniques is just the first step. The United States is constitutionally committed to protecting freedom of expression on the internet in ways that many other countries are not. Some countries wish to have complete control of the traffic on the internet. They see freedom of speech as a threat to their power and the Dark Web as a tool that enables dissidents to speak freely. The internet is by its nature an international network of computers. Enforcement jurisdiction is foggy at best, so governments must find ways to cooperate in establishing at least some mutually agreeable regulations that govern the Dark Web.

The debate surrounding the Dark Web is by no means over. Online anonymity is a double-edged sword that must be handled delicately. As policy-makers move forward, they must monitor vigilantly the evolution of the Dark Web and ensure that enforcement agencies have the resources and legal support to police successfully the Dark Web. Dark Web policy, like all good policy, must be nuanced and thoughtful in order to strike the balance between the needs of privacy-minded users and the government's responsibility to stop illegal activity.

Acknowledgements

The author would like to thank Eric Karsten for his research and help in preparing this article.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Michael Chertoff served as a Secretary of the U.S. Department of Homeland Security from 2005 to 2009. He led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organisation following Hurricane Katrina. His greatest successes have earned few headlines – because the important news is what did not happen.

At Chertoff Group, Mr Chertoff serves as the Co-Founder and Executive Chairman where he provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response, and recovery. 'Risk management has become the CEO's concern,' he says. 'We help our clients develop comprehensive strategies to manage risk without building barriers that get in the way of carrying on their business.'

Before heading up the Department of Homeland Security, Mr Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organised crime, corporate fraud and terrorism – including the investigation of the 9/11 terrorist attacks.

Mr Chertoff is a magna cum laude graduate of Harvard College (1975) and Harvard Law School (1978). From 1979–1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

In addition to his role at Chertoff Group, Mr Chertoff is also senior of counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

References

Clemmitt, M. 2016. "The Dark Web." Accessed August 30, 2016. http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016011500.

Cox, J. 2016. "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers." Accessed August 30, 2016. https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

Darknet Markets Are Not beyond the Reach of Law. 2016. Accessed August 30, 2016. https://darkwebnews.com/darknet-markets/darknet-not-beyond-law/.

Finklea, K. 2015. "Dark Web." Accessed August 30, 2016. https://www.fas.org/sgp/crs/misc/R44101.pdf.

Going Dark: The Internet behind the Internet. 2014. Accessed August 30, 2016. http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet.

Greenberg, A. 2014. "Hacker Lexicon: What is the Dark Web." Accessed August 30, 2016. https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

Jardine, Eric. 2015. "The Dark Web Dilemma: Tor, Anonymity and Online Policing." Accessed December 14, 2016. https://www.cigionline.org/sites/default/files/no.21.pdf.

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2013. "How Censorship in China Allows Government Criticism but Silences Collective Expression." Accessed December 13, 2016. http://gking.harvard.edu/files/gking/files/censored.pdf.

Owen, Gareth and Nick Savage. 2015. "The Tor Dark Net." Accessed December 13, 2016. https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf.

Satterfield, J. 2016. "FBI Tactic in National Child Porn Sting under Attack." Accessed September 6, 2016. http://www.usatoday.com/story/news/nation-now/2016/09/05/fbi-tactic-child-porn-sting-under-attack/89892954/.

Stevens, G. n.d. "The Truth about the Deep Web." Accessed August 30, 2016. http://kernelmag.dailydot.com/features/report/7477/the-truth-about-the-deep-web/.

Sui, D., J. Caverlee, and D. Rudesill. 2015. "The Deep Web and the Darknet." Accessed August 30, 2016. https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet.

Swearingen, J. 2014. "A Year after Death of Silk Road, Darknet Markets are Booming." Accessed August 30, 2016. https://finance.yahoo.com/news/death-silk-road-darknet-markets-142500702.html.

Tor: Sponsors. n.d. Accessed August 30, 2016. https://www.torproject.org/about/sponsors.html.en.

Vitaris, B. 2015. "Russian Government Sues Firm for Failing to Deanonymize Tor Users." Accessed August 30, 2016. https://www.deepdotweb.com/2015/11/30/russian-government-sues-firm-failing-deanonymize-tor-users/.

Vitaris, B. 2016. "Russian [Sic] is Collecting Encryption Keys as 'Anti-terrorism' Legislation Goes into Effect." Accessed August 30, 2016. https://www.deepdotweb.com/2016/08/03/russian-collecting-encryption-keys-anti-terrorism-legislation-goes-effect/.

Ward, M. 2014. "Tor's Most Visited Hidden Sites Host Child Abuse Images." Accessed August 30, 2016. http://www.bbc.com/news/technology-30637010.

Yellin, T., D. Aratari, and J. Pagliery. n.d. What is Bitcoin? Accessed August 30, 2016. http://money.cnn.com/infographic/technology/what-is-bitcoin/.