9-14-2020

Investigating Dark Net Criminals and the Resulting Legal Consequences

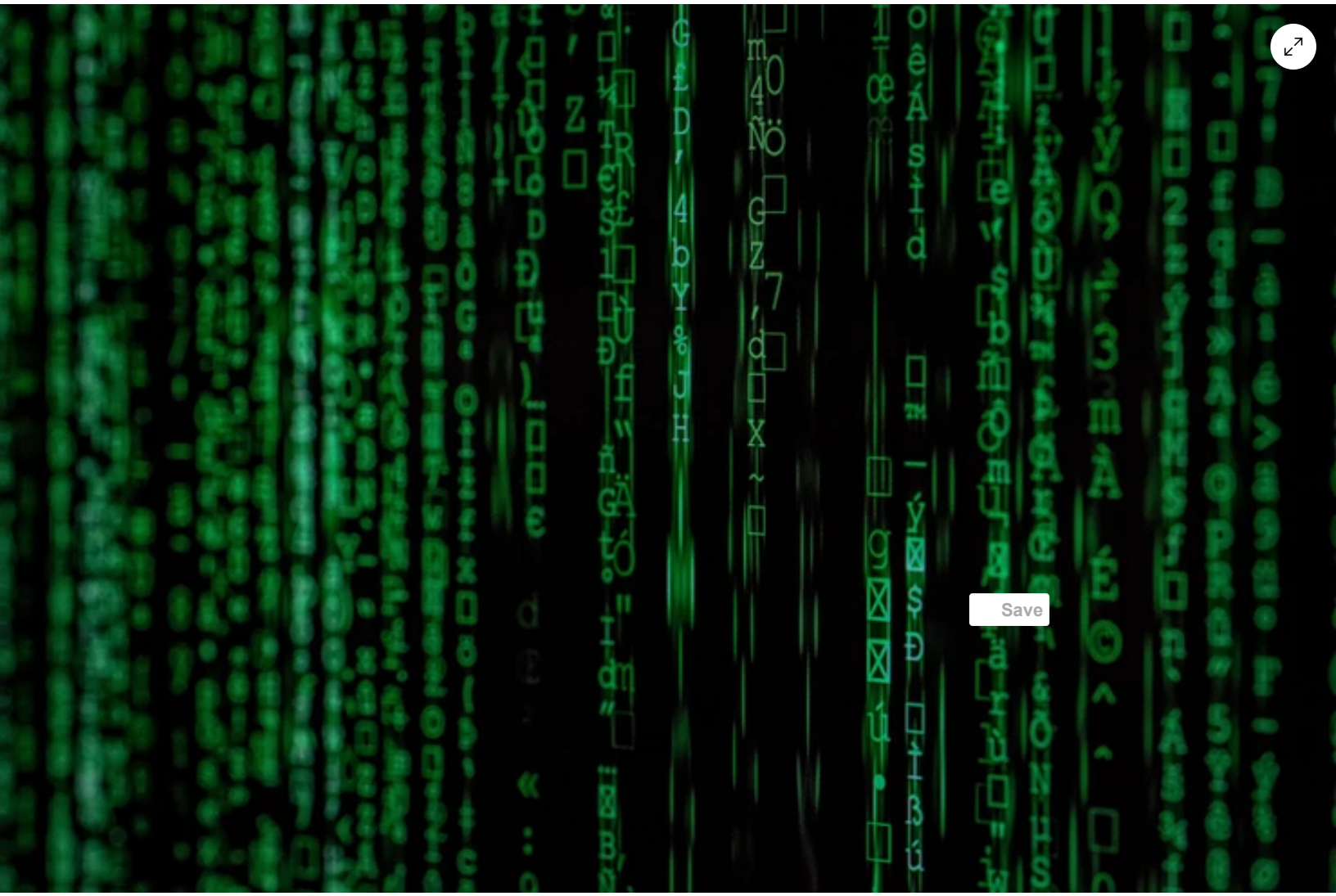
Alec Kirschenbaum
Cardozo International & Comparative Law Review, akirsche@law.cardozo.yu.edu

CICLR Sep 14, 2020 6 min read

Investigating Dark Net Criminals and the Resulting Legal Consequences

Updated: Sep 28, 2020

*By: Alec Kirschenbaum**



When most people think of the Internet, what they are referring to is what is known as the "Surface Web." The Surface Web is made up of websites that are indexed by traditional search engines like Google, Bing, Yahoo, and Firefox.[1] For instance, when an individual searches for something on Google, he or she is using and accessing the information through the Surface Web. A majority of traditional Internet users believe that they have full access to all of the information available on the Web, but this belief is erroneous. In fact, it has been suggested and estimated by researchers, that the Surface Web only makes up 1 to 16 percent of all the information available on the Web. [2] The rest of the Web is comprised of websites found on either the "Deep Web" or the "Dark Net."[3]

Unlike the Surface Web, websites on the Deep Web are not indexed. As such, they are not easily accessible by the average Internet user.[4] Many of the websites found on the Deep Web are databases; for instance, the U.S. Census Bureau, Securities and Exchange Commission, and Patent Trademark Office all have their databases on the Deep Web.[5] With that said, the Deep Web is made up of "private networks, like those operated by companies, [and] universities."[6] Similar to websites found on the Deep Web, Dark Net websites are not indexed by traditional search engines. However, the difference between the two is that Dark Net websites are "anonymously-hosted and are only accessible with special software and browsers that mask one's I.P. address."[7] Therefore, the only way a person can access a website on the Dark Net is by using a special browser called Tor.[8] Tor works by "rout[ing] internet traffic through a series of nodes, which consist of computers hosted on the Tor network by volunteers. The process of randomly bouncing data through many different nodes makes it nearly impossible to trace the data back to [any one] internet user."[9] The Naval Research Laboratory originally developed Tor in the 1990s.[10] According to the Tor Project, the original purpose, held by the founders, was to create a way of communicating "without reveal[ing] who is talking to whom, even to someone monitoring the network."[11]

Today, in certain aspects, Tor has moved away from its intended purpose of providing a means of communicating anonymously over the Internet. As studies have shown, "the most common uses for websites on Tor hidden services are criminal, including [dealings with]drugs, illicit finance and pornography involving violence, children and animals."[12]

Prior to October 2013, most people had never heard the term "Dark Net" before, but that suddenly changed when Ross William Ulbricht was arrested in San Francisco for, essentially, creating and operating a Dark Net website called the Silk Road.[13] The Silk Road was a criminal marketplace where people were able to purchase and sell an array of illegal items and services.[14] Some of these items and services consisted of the following: drugs, false identification documents, and computer hacking services.[15] "According to the government, between 2011 and 2013, thousands of vendors used Silk Road to sell approximately $183 million worth of illegal drugs, as well as other goods and services."[16] Ultimately, Ulbricht was convicted by a jury for drug trafficking and other crimes stemming from his creation and involvement with the Silk Road.[17] His conviction was later affirmed in 2017.[18]

The investigation into Ulbricht's involvement and operation of the Silk Road sparked controversies over the ethical and constitutional violations surrounding methods used by law enforcement agents to connect Ulbricht to the website. In 2011, when the Silk Road was created, law enforcement agencies took notice. However, they had no idea who the mastermind was behind the site. In Ulbricht's appeal, the court does not specify how Ulbricht became a suspect, and that lack of transparency is beyond the scope of this piece.

However, when Ulbricht became the main suspect in the investigation, "the government obtained five 'pen/trap' orders" under 18 U.S.C. §§ 3121-27.[19] These orders allowed the government to collect IP address information from the internet "traffic to and from Ulbricht's home wireless router and other devices that regularly connected to Ulbricht's home router."[20] As the court explained in Ulbricht's appeal, an IP address is a special number that identifies the device that is connected to the Internet. As the court explained, "an 'IP address is analogous to a telephone number' because 'it indicates the online identity of the communicating device without revealing the communication's content."[21]
Ulbricht argued that the use of the Pen/Trap orders violated his Fourth Amendment rights because it helped link him to the Silk Road by getting access to his home Internet data.[22] The implementation and use of Pen/Trap orders does not require search warrants. Rather, the statute only requires "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[23] This low standard has attracted many law students and scholars to write about the constitutionality surrounding the statute. As one author put it, the use of Pen/Trap orders are alarming because "'the court will not conduct an independent judicial inquiry into the veracity of the attested facts.' The statute does not require the agency seeking access to describe what types of 'dialing, routing, addressing signaling information' it intends to collect."[24] As the government does not have to specify what information it intends to collect, an average person might face unnecessary intrusion from the government via a Pen/Trap order because the government can claim the information is relevant to a criminal investigation. Additionally, in the Note, "Incognito Mode is in the Constitution," the author concludes by suggesting that that the approach laid out in *Carpenter* "should apply to law enforcement's collection of non-content internet history and subscriber information."[25] Therefore, it is fair to say that the methods used to unmask and identify criminals hiding in the shadows of the Dark Net present numerous privacy concerns and some sort of reform is in order.

However, there is another problem that most law students and legal scholars fail to recognize when combatting Dark Net criminals. The problem remains that if methods like Pen/Trap orders and Network Investigative Techniques (not discussed in this piece) are continued to be used, then Tor might become obsolete. One might wonder why that is a problem. The answer is simple: Tor provides numerous benefits. For instance, not every country enjoys the same censorship freedoms that the United States provides. Some countries "go as far as to limit the access of information such as news and suppress discussion among citizens. Internet censorship also occurs in response to or in anticipation of events such as elections, protests, and riots."[26] If a particular country does not allow its citizens to access Facebook or a website like the BBC, then a person can turn to Tor to access those sites because Tor changes the person's IP address.[27] In addition, Tor and the Dark Net allow people, all around the world, to share their social and political beliefs limiting their risk of facing penalties from their prospective governments.[28] While it was mentioned above that many users of the Dark Net, use it as a means of carrying out illegal activities, a study was conducted and 12 out of 17 of the individuals "stated that 'anonymity' and 'freedom' are the two main reasons behind their initial and continued use of the Darknet."[29] This indicates that there are social and political benefits to using Tor and the Dark Net.

In sum, while the Ulbricht case illustrates the need for both policing the Dark Net and reforming the techniques used by law enforcement agencies due to privacy and constitutional concerns, the United States and the International community as a whole needs to understand the benefits that the Dark Net provides.

** Alec is a 2L at Benjamin N. Cardozo School of Law interested in the legal implications of technology on developing nations and the international community. He earned his undergraduate degree in Political Science with a minor in Middle Eastern & North African Studies from Rollins College.*

---

[1] B.J. Altvater, Combatting Crime on The Dark Web 21 (2016), https://pceinc.org/wp-content/uploads/2019/11/20161219-Combatting-Crime-on-the-Dark-Web-How-Law-Enforcement-and-Prosecutors-are-Using-Cutting-Edge-Technology-to-Fight-Cyber-Crime-PCE-Altvater.pdf.
[2]Sophia Dastagir Vogt, *The Digital Underworld: Combatting Crime on the Dark Web in the Modern Era*, 15 Santa Clara J. Int'l L. 104, 109 (2017); *see also id*.
[3]*See supra* note 1.
[4]*Id.*
[5]*Id.*
[6]*Id.*at 21.
[7]*Id.*
[8] *See* Vogt, *The Digital Underworld*, *supra* note 2, at 15.
[9]*See*Altvater, *supra*note 1, at 21
[10]*Id.*at 21.
[11] Tor Project, https://www.torproject.org/about/history/(last visited Sept. 12, 2020).
[12]Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, 58 Survival7, 21 (2016), https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true.

[13]United States v. Ulbricht, 858 F.3d 81, 82-83 (2nd Cir. 2017).
[14]*Id.*
[15]*Id.*
[16]*Id.*at 83.
[17]*Id.*
[18]*Id*. at 135.
[19]*See supra* Ulbricht note 13, at 83.
[20]*Id.*
[21]*Id.*
[22]*Id.*at 84.
[23]18 U.S.C.A. § 3122 (West 1986) (Application for an order for a Pen Register or a Trap and Trace Device).
[24]Kyriaki Council, *Emotional Abrogation: How Internet Child Pornography Prosecution Impacts Search and Seizure of Computers in Other Crimes*, 15 Colo. Tech. L. J.435, 447 (2017).
[25]Travis Panneck, *Incognito Mode is in the Constitution*, 104 Minn. L. Rev. 511, 513 (2019).
[26]Khristal Thomas, *Is the Dark Web Going Commercial? Internet Censorship May Be Driving the Trend*, GeorgetownGeorgetown Pub. Pol.R.(Mar. 6, 2020), http://gppreview.com/2020/03/06/dark-web-going-commercial-internet-censorship-may-driving-trend/.
[27]*Id.*
[28]Mirea, et al., *The Not so Dark Side of the Darknet: a Qualitative Study*,SpringerLink(2018), https://link.springer.com/article/10.1057/s41284-018-0150-5.
[29]*Id.*