COMBATTING CRIME ON THE DARK WEB

HOW LAW ENFORCEMENT AND PROSECUTORS ARE USING CUTTING-EDGE TECHNOLOGY TO FIGHT CYBER CRIME

PROSECUTORS' CENTER FOR EXCELLENCE

December 2016

Combatting Crime on the Dark Web:

How Law Enforcement and Prosecutors are Using Cutting Edge Technology to Fight Cybercrime

COMBATTING CRIME ON THE DARK WEB:
HOW LAW ENFORCEMENT AND PROSECUTORS ARE USING CUTTING EDGE TECHNOLOGY TO FIGHT CYBERCRIME[1]

Introduction

Criminals are increasingly using shadowy corners of the internet to mask their identities and conduct illicit activities. Marketplaces on the "dark web" facilitate a range of criminal activities, including human trafficking and the distribution of child pornography. However, law enforcement and prosecutors are not helpless in the fight against these new criminal tactics. This paper will focus on two ways that law enforcement and prosecutors have utilized technology to find and prosecute criminals on the dark web. Part 1 of this article explains this new terrain of criminal activity by exploring the differences between the surface web, deep web, and dark web. Part 2 explores the use of Network Investigative Techniques (NITs) to pierce the anonymity of criminals on the dark web. Finally, Part 3 discusses a new toolkit of programs that can help investigators combat human trafficking with data-mining of the dark web.

Part 1 - What is the Difference between the Surface Web, Deep Web, and Dark Web?

The average person interacts with the internet on what is referred to as the "surface web." The common definition of the surface web is all web pages that are indexed by normal search engines (e.g. Google, Yahoo, or Bing). Search engines index web sites by following the links to all available sites and mapping out the web of connections.[2] For example, social media, news sites, and online retailers all exist on

[1] The author of this article is Georgetown Law student, B. J. Altvater. The article was written as part of the Best Practices for Justice Prosecutor Practicum at Georgetown Law School. Specific thanks go to John Temple, Assistant District Attorney in charge of the Human Trafficking Program in the New York County District Attorney's Office for his insights and comments. Additional thanks go to Kristine Hamann, Executive Director of Prosecutors' Center for Excellence (PCE) and Adjunct Professor for the Prosecutor Practicum, as well as Jessica Trauner, Consulting Attorney with PCE, who both assisted with the article.

[2] Jose Pagliery, *The Deep Web You Don't Know About*, CNN MONEY (Mar. 10, 2014), http://money.cnn.com/2014/03/10/technology/deep-web/index.html.

the surface web. According to one study, the surface web contains over 4 billion indexed web sites.[3]

As big as that sounds, many experts believe that the surface web makes up less than 1% of the internet.[4] The much larger part of the internet is made up of content that is not indexed and is referred to as the "deep web." One large source of deep web content is databases.[5] Some very large databases on the deep web are available to the public, such as those hosted by the U.S. Census Bureau, Securities and Exchange Commission, and Patent and Trademark Office. Other databases are owned by companies (e.g. LexisNexis and Westlaw) that charge a fee to access the content.[6] Another large source of content on the deep web is private networks, like those operated by companies, universities, or government agencies.[7]

The "dark web" is similarly made up of sites that are not indexed by search engines. However, websites on the dark web are also anonymously-hosted and are only accessible with special software and browsers that mask one's IP address.[8] The most common tool to navigate the dark web is the Tor (The Onion Router) browser.[9] Tor routes internet traffic through a series of "nodes," which are 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 an internet user.[10] In fact, the U.S. Naval Research Laboratory initially developed Tor as a way to secure communications.[11]

While the dark web was not designed to facilitate criminal enterprises, law enforcement and prosecutors are increasingly facing legal challenges involving anonymous services online. In fact, one recent study revealed, "the most common

---

[3] THE SIZE OF THE WORLD WIDE WEB (THE INTERNET), http://www.worldwidewebsize.com (last visited Oct. 30, 2016).

[4] Pagliery, *supra* note 1.

[5] *Id*.

[6] *Id*.

[7] *Id*.

[8] Cadie Thomspson, *Beyond Google: Everything You Need to Know About the Hidden Internet*, TECH INSIDER (Nov. 25, 2015), http://www.techinsider.io/difference-between-dark-web-and-deep-web-2015-11.

[9] *Id*.

[10] Tor Project, https://www.torproject.org/about/overview.html.en (last visited Oct. 30, 2016).

[11] Geoffrey A. Fowler, *Tor: An Anonymous, And Controversial, Way to Web-Surf*, THE WALL STREET JOURNAL (Dec. 12 2012), http://www.wsj.com/articles/SB10001424127887324677204578185382377144280; *see also* Damon McCoy et al., *Shining Light in Dark Places: Understanding the Tor Network*, UNIVERSITY OF COLORADO, BOULDER, CO, http://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf.

uses for websites on Tor hidden services are criminal, including drugs, illicit finance and pornography involving violence, children and animals."[12]

Part 2 - How can Prosecutors and Law Enforcement Use Network Investigative Techniques (NITs) on the Dark Web?

Criminal actors and organizations are increasingly relying on the anonymity provided by the dark web to host web sites that traffic illicit materials and content. One way that law enforcement and prosecutors are able to pierce the dark web's cloak of anonymity is by employing a network investigative technique (NIT). Operation Pacifier is a recent example where the FBI and DOJ employed an NIT to find and prosecute criminals operating on the dark web. While the use of NITs has been limited to federal law enforcement, state and local law enforcement agencies with advanced cyber capabilities may employ this tactic in the future.

What is Operation Pacifier?

In August 2015, a new website called "Playpen" appeared on the dark web. Playpen's focus was "the advertisement and distribution of child pornography," and this new site allowed users to post images.[13] The site had almost 60,000 accounts registered in its first month and nearly 215,000 accounts by 2016.[14] Playpen hosted over 117,000 posts with 11,000 visitors per week, and much of the content included "some of the most extreme child abuse imagery one could imagine."[15] The FBI described Playpen as "the largest remaining known child pornography hidden service in the world."[16]

In February 2015, the FBI seized the server running Playpen from a web host in Lenoir, North Carolina.[17] However, the FBI did not immediately shut the site

---

[12] Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, SURVIVAL: GLOBAL POLITICS AND STRATEGY 21 (Feb. 1, 2016) http://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true.

[13] Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, MOTHERBOARD (Jan. 5, 2016) https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

down.[18] Instead, the FBI operated the site from its own servers in Virginia from February 20th to March 4th.[19] While the FBI maintained control of Playpen during this period, law enforcement officers were able to deploy a network investigative technique (NIT) to identify, and later prosecute, users of the site.[20]

The FBI's efforts to take control of Playpen's servers, deploy an NIT (i.e. a hacking tool) to identify users, and then prosecute individuals on child pornography charges became known as Operation Pacifier.[21] Currently, the Department of Justice has publicly acknowledged, "at least 137 cases have been filed in federal court as a result of this investigation."[22] An FBI special agent explained in one court that "The NIT was deployed against users who accessed posts in the 'Preteen Videos—Girls Hardcore' forum because users accessing posts in that forum were attempting to access or distribute or advertise child pornography."[23] Additionally, Judge Robert J. Bryan has stated "The FBI setup the NIT so that accessing the forum hyperlink, not Website A's [Playpen] main page, triggered the automatic deployment of the NIT from a government-controlled computer in the Eastern District of Virginia."[24]

What is a Network Investigative Technique (NIT)?

Playpen's existence in the dark web meant that the locations of both its servers and the computers accessing the site were concealed. As discussed above, users could only access the site via the Tor browser, which anonymized user traffic. As part of Operation Pacifier, the FBI successfully located the Playpen server and gained control. However, the FBI still was not able to identify the locations of individuals who were posting or consuming child pornography on the web site through Tor.[25] In

---

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, MOTHERBOARD (Jul. 27, 2016), https://motherboard.vice.com/read/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen.

[22] *Id.*

[23] Joseph Cox, *FBI: Hacking Tool Only Targeted Child Porn Visitors*, MOTHERBOARD (Jul. 29, 2016), https://motherboard.vice.com/read/fbi-hacking-tool-only-targeted-child-porn-visitors.

[24] *Id.*

[25] Susan Hennessy & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (Jul. 28, 2016, 10:17 AM), https://lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques.

order to determine the Playpen users IP addresses, the FBI employed a court-authorized hacking method referred to as an NIT.[26]

An NIT consists of four main components: (1) a generator, (2) an exploit, (3) a payload, and (4) a logging server. A generator runs on the "hidden service" (e.g. Playpen) and produces a unique identification (ID) number that is associated with each user of the dark web site. The generator then transmits that unique ID, along with the exploit and payload, to each user's own computer. Once on a user's computer, the exploit takes control of the Tor browser (i.e. hacks) and executes the payload. The details of exactly how the exploit works is "the most sensitive part of an NIT – public disclosure not only risks losing the opportunity to use the technique against other offenders but would also permit criminals or authoritarian governments to use it for illicit purposes until a patch is developed and deployed."[27]

Next, the payload searches a user's computer for those materials authorized in a search warrant. Relevant information would likely include the individual's username, the unique identifying number of the computer's network card (i.e. MAC address), and the computer's name. After identifying this information, the payload sends it to the logging service and creates a record of the computer that the user used to access the dark web site. This process also allows the payload to capture the public IP address of the user's computer. The logging service records all of the information sent from the payload on a separate computer at the FBI.[28]

The FBI can then use the IP addresses to serve a subpoena on an internet service provider, which will provide the government with a user's name and physical address. Armed with probable cause that the user accessed illegal content, the FBI then obtains a search warrant for the user's computer. By seizing the computer, the government is able to prove that the same computer with that NIT accessed the dark web site.[29]

What Are the Key Legal Defenses to Operation Pacifier Prosecutions?

Two common defense strategies have unfolded from the current prosecutions of individuals identified by FBI's use of an NIT under Operation Pacifier: (1) compel

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

the government to disclose the NIT's sensitive exploit code, and (2) challenge the warrant as fundamentally flawed.[30]

"Disclose or Dismiss"

One defendant charged as part of Operation Pacifier was able to keep evidence out of court by requesting all of the source code for the NIT. Jay Michaud, a public school administrator in Vancouver, Washington, was arrested in July 2015 as part of the FBI's investigation and deployment of an NIT involving the Playpen web site.[31] Michaud's attorneys requested the course code for the NIT, which they argued they needed in order to understand how the government identified their client.[32]

The government initially turned over an incomplete version of the NIT code, but the defense believed that critical pieces were missing.[33] Michaud's attorneys argued they needed the part of the code that could determine whether the NIT-produced identifier assigned to Michaud's computer was, in fact, unique.[34] Michaud's team also requested the exploit code that was used to bypass his web browser because, they argued, they needed the exploit details to ensure that the NIT did not engage in any actions beyond the government's description of the code.[35]

The government responded by stating that defendant's discovery request of the NIT source code had no bearing on the large amounts of child pornography that the FBI found on Michaud's thumb drives and cell phone.[36] However, Judge Robert J. Bryan of the Western District of Washington disagreed, and he ordered the government to turn over the full NIT source code, stating:

> "Much of the details of this information is lost on me, I am afraid, the technical parts of it, but it comes down to a simple thing … You say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question … The government should respond under

---

[30] Cox, *supra* note 20.

[31] Joseph Cox, *Transcript Shows Why a Judge Ordered the FBI to Reveal Its Mass Hacking Malware*, MOTHERBOARD (Feb. 24, 2016), http://motherboard.vice.com/read/transcript-shows-why-a-judge-ordered-the-fbi-to-reveal-mass-hacking-malware-playpen-jay-michaud.

[32] *Id*.

[33] *Id*.

[34] *Id*.

[35] *Id*.

[36] *Id*.

seal and under the protective order, but the government should respond and say here's how we did it."[37]

In response, the Department of Justice filed a sealed motion asking the judge to reconsider.[38] An FBI agent involved in Operation Pacifier also provided a public statement where he rebuffed the defendant's rationale for requesting the entire NIT source code.[39] He explained, "Discovery of the 'exploit' would do nothing to help [the defense] determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Michaud's computer, not what it did once deployed."[40] He continued, "Determining whether the government exceeded the scope of the warrant thus requires an analysis of the NIT instructions delivered to Michaud's computer, not the method by which they were delivered."[41]

However, Judge Bryan still ruled that the defendant was entitled to see the NIT exploit code under a protective order. As discussed above, the exploit code details how the FBI was able to circumvent the privacy protections built into the Tor Browser and is the most sensitive part of the NIT. In the case against Michaud, the DOJ ultimately refused to produce the information for Michaud, and Judge Bryan suppressed the evidence.[42] The FBI and DOJ attorneys concluded that disclosure of the NIT exploit code, even under a protective order, involved too great a risk to continue the case against Michaud.

Challenging the Search Warrant

Another defense successfully employed by an Operation Pacifier defendant, Alex Levin, is to challenge the search warrant for the NIT.[43] Defendants have successfully challenged the validity of the search warrant under two theories: (1) the

---

[37] *Id.*

[38] Joseph Cox & Sarah Jeong, *FBI Is Pushing Back Against Judge's Order to Reveal Tor Browser Exploit*, MOTHERBOARD (Mar. 29, 2016), https://motherboard.vice.com/read/fbi-is-pushing-back-against-judges-order-to-reveal-tor-browser-exploit.

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] Joseph Cox, *A Judge Just Made It Harder for the FBI to Use Hacking*, MOTHERBOARD (May 25, 2016), https://motherboard.vice.com/read/playpen-tor-browser-exploit.

[43] United States v. Levin, NO. 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016) (order suppressing evidence).

warrant is overly broad, and (2) the warrant is in violation of Rule 41 of the Federal Rules of Criminal Procedure.

A key argument for challenging the validity of the NIT warrant is that it was overly broad. Specifically, legal opponents point out that the NIT warrant enabled the FBI to deploy its payload (i.e. hack) to any "activating computer," which would be any computer that logged on the target site. That means that the warrant did not specify exactly which computers would be searched, to whom they belonged to, or even where the systems were physically located. Thousands of users visited Playpen during the two-week period that the FBI maintained control of the site, and those users were located all over the world.[44]

In an amicus brief filed against the NIT warrant used in Operation Pacifier, the Electronic Frontier Foundation (EFF) argued that the warrant was unconstitutional and stated:

> "The Warrant here did not identify any particular person to search or seize. Nor did it identify any specific user of the targeted website. It did not even attempt to describe any series or group of particular users. Similarly, the Warrant failed to identify any particular device to be searched, or even a particular type of device. . . . Compounding matters, the Warrant failed to provide any specificity about the place to be searched – the location of the "activating computers."[45]

Attorneys for defendant Alex Levin argued in the District of Massachusetts that the warrant issued in the Eastern District of Virginia was overly broad and fundamentally flawed.[46] One defense attorney argued that the NIT warrant "effectively authorize[d] an unlimited number of searches, against unidentified targets, anywhere in the world."[47] Judge William G. Young of the District of Massachusetts agreed with Levin's defense and excluded all of the evidence gathered by the use of the NIT.[48] He stated, "Based on the foregoing analysis, the Court concludes that the NIT warrant was issued without jurisdiction and thus was void *ab initio*. It follows that

---

[44] Andrew Crocker, *Why the Warrant to Hack in the Playpen Case Was an Unconstitutional General Warrant,* ELECTRONIC FRONTIER FOUNDATION (Sep. 28, 2016), https://www.eff.org/deeplinks/2016/09/why-warrant-hack-playpen-case-was-unconstitutional-general-warrant.

[45] *Id*.

[46] Joseph Cox, *In a First, Judge Throws Out Evidence Obtained from FBI Malware,* MOTHERBOARD (Apr. 20, 2016), https://motherboard.vice.com/read/in-a-first-judge-throws-out-evidence-obtained-from-fbi-malware.

[47] *Id*.

[48] *Id*.

the resulting search was conducted as though there were no warrant at all."[49] Despite Judge Young's ruling, judges of Playpen cases proceeding in other jurisdictions have not yet applied similar reasoning.

In addition to the claim that that the NIT warrant was unconstitutional, defendants have also argued that the warrant violated Rule 41 of the Federal Rules of Criminal Procedure.[50] Rule 41 authorizes magistrate judges, with few exceptions, to issue search warrants only in the judge's *own* judicial district. The "territorial" requirement helps to protect against law enforcement seeking out a sympathetic judge, who has no connection to the judicial district, in order to obtain search warrants.[51]

Opponents of the NIT warrant argued that the magistrate judge who granted the warrant in the Eastern District of Virginia violated the Rule 41 territorial requirement by authorizing a search of *any* computer that accessed Playpen.[52] Prior to obtaining the warrant and deploying the NIT, the FBI would not have been able to determine the locations of users accessing Playpen via the Tor browser.[53] Thus, since the FBI was unable determine where the search would take place (or at least the judicial district), opponents argued that the warrant ran afoul of Rule 41.[54]

In April of 2016, the Supreme Court approved a change to the existing Rule 41 that would allow federal judges to issue search warrants that target computers outside their judicial district.[55] A panel of federal judges drafted the new version of the rule at the request of the Department of Justice, and Chief Justice Roberts submitted the rule to Congress as part of the Court's annual amendments to the Federal Rules of Criminal Procedure.[56] The change to Rule 41 would permit a magistrate judge to issue a warrant, like the Operation Pacifier NIT warrant, to hack into computers and seize

---

[49] *Id*.

[50] *See* FED. R. CRIM. P. 41.

[51] Mark Rumold, *The Playpen Story: Rule 41 and Global Hacking Warrants*, ELECTRONIC FRONTIER FOUNDATION (Sep. 26, 2016), https://www.eff.org/deeplinks/2016/08/illegal-playpen-story-rule-41-and-global-hacking-warrants.

[52] *Id*.

[53] *Id*.

[54] *Id*.

[55] Matt Ford, *The Supreme Court Expands FBI Hacking Powers*, THE ATLANTIC (Apr. 29, 2016), http://www.theatlantic.com/politics/archive/2016/04/supreme-court-fbi-hacking/480498/.

[56] *Id.*

data outside the judge's jurisdiction when the computer's physical location "has been concealed through technical means."[57]

Part 3 - Data-Mining and the Dark Web

The vast quantity of data on the internet frequently challenges investigators trying to find information relevant to an investigation. Investigators face an even greater challenge on the dark web, where information on criminal enterprises is located in obscure advertisements or on hidden service websites. However, one new data-mining toolkit, called Memex, is enabling investigators to find critical information. Some investigators are already utilizing this new toolkit to combat human trafficking on the dark web.

What is MEMEX?

Anonymity on the dark web enables a wide range of criminal activities to flourish. Human trafficking is one illegal activity that takes advantage of anonymous buying and selling on the dark web's hidden service web sites.[58] Even a human trafficker still needs to tell potential customers how to find his hidden site, though.[59] As discussed above, web sites on the dark web are not indexed by the major search engines, so the illicit sites would not show up in the results of a Google search.[60] To drive traffic, human traffickers on the dark web often use one-off advertisements in social posts and chat rooms that usually only contain photos and code words commonly associated with the sex trade.[61] This advertising tactic makes it very difficult for law enforcement to find and track individuals engaged in human trafficking.[62]

However, one program manager at the Defense Advanced Research Projects Agency (DARPA)[63] came up with a way to make it easier to find human traffickers on

---

[57] *Id.* The new rule will go into effect on December 1, 2016 unless Congress passes legislation to override the proposed change by the Court. *See id.*

[58] Charles Graeber, *The Man Who Lit the Dark Web*, POPULAR SCIENCE (Aug. 30, 2016), http://www.popsci.com/man-who-lit-dark-web.

[59] *Id.*

[60] *See supra* Part I (A).

[61] Graeber, *supra* note 66.

[62] *Id.*

[63] DARPA is part of the Department of Defense. The organization's mission is "to make pivotal investments in breakthrough technologies for national security." DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, http://www.darpa.mil/about-us/about-darpa.

the dark web.[64] Chris White, a program manager at DARPA, had experience building tools for mining big data and visualizing the results while supporting the military in Afghanistan.[65] He later used that experience to lead a project at DARPA aimed at building a suite of search-engine tools that would enable users [e.g. law enforcement] to find, interact with, and understand data available on the surface web, deep web, *and* dark web.[66] White and his team called this suite of applications Memex, a combination of "memory" and "index."[67]

DARPA decided to test Memex by giving it to certain law enforcement agencies to combat human trafficking.[68] Many parts of the Memex suite of tools have direct applications to help investigators find sex traffickers. One of the first tools utilized by law enforcement was called "Datawake." Although the functions of Datawake have since been absorbed into other Memex tools, the program originally helped law enforcement to find and organize relevant data from an otherwise overwhelming amount of data. For example, a law enforcement officer may have had an email address or phone number for a known prostitute. A standard Google search of that one email or phone number would likely result in thousands of hits, and almost all of those hits would be irrelevant. Looking through all of the thousands of search results in order to find a few useful tips would overwhelm investigators.[69]

However, the same law enforcement officer was able to use Datawake to search through all of those same Google results and organize it visually with different lines and circles showing the connections between different pieces of information. After seeing the results in Datawake, officers were able to see other names, phone numbers, or photos that repeatedly link to the original email or phone number. These connections, in turn, greatly aided law enforcement to pursue relevant leads without getting lost in a sea of data. Datawake also enabled investigators to review prior cases and search the phone numbers, emails, and addresses used as evidence in sex crime prosecutions. The tool even revealed additional information that helped build new

[64] Graeber, *supra* note 66.

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] *Id*.

[69] *Id*.

cases of criminal conspiracy by linking individuals already in prison to existing human trafficking operations.[70]

"TellFinder" is a very useful current program in the Memex toolkit. Tellfinder retrieves co-referenced information from sex ads on the internet and organizes the commonalities. By examining these commonalities in the ads, investigators are able to identify groups that are likely by the same author. As an example, a law enforcement officer could pull hundreds of thousands of current sex ads from the internet and TellFinder would populate them as bubbles on a map display of the U.S. Once displayed, the officer could then zoom in on a particular jurisdiction and then scroll to show how the sex ads were posted over time. The map display also shows common pieces of information in the ads (e.g. phone numbers, emails, and addresses), and the program even has the capability to recognize photos that contain the same background. Additionally, the officer could also track the sex ads for a particular woman over time as a way to identify the track of how she was being trafficked around the country.[71]

"Dig" is another very useful tool that takes that co-referenced information pulled by TellFinder and sorts it into a very organized list - a list similar to one you would get from a search on Amazon. Dig displays different categories and key terms along the side of the results, so an investigator can further hone and filter searches. Dig also has the ability to perform some even more advanced photo commonality searches than in TellFinder.[72]

Finally, "Aperture Tiles" is another powerful tool that "makes formerly unmanageable amounts of information— think billions of moving data points on a map—manageable."[73] As an example, Aperture Tiles can compare the addresses associated with the sex trade (e.g. certain motels) with the location information associated with social media posts. Many posters are unaware that the location feature of an application is enabled, providing valuable geographic information on where a particular sex ad was actually posted. By analyzing this data through Aperture Tiles, law enforcement officers can identify patterns of how sex traffickers are moving around a particular city. The tool can also help to identify how certain traffickers operate in one city for a few days before moving on to a new location. Law

---

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *Id.*

enforcement can even use the tool to show an international nexus, as Aperture Tiles has demonstrated that some known traffickers are frequently located in Southeast Asia.[74]

How Have Prosecutors Used Memex to Prosecute Human Traffickers?

The DARPA team, which began testing Memex with law enforcement in 2014, has continued to introduce the platform to district attorney's offices, law enforcement, and non-governmental organizations (NGOs).[75] The New York Police Department and Manhattan District Attorney's Office's (DANY) Human Trafficking Response Unit have employed Memex, since January 2014.[76] Today, DANY uses Memex in every human trafficking case, and investigators screened 4,752 potential cases in the first six months of 2016.[77] Manhattan District Attorney Cyrus Vance described his office's use of Memex:

> "We cannot rely on traumatized victims alone to testify in these complex cases. When sex traffickers create online ads for their victims' sexual services, they leave a digital footprint that leads us to their criminal activity. Because those ads are frequently removed or intentionally hidden on the 'dark web,' it puts them beyond the reach of typical search engines, and therefore, beyond the reach of law enforcement. With technology like Memex, we are better able to serve trafficking victims and build strong cases against their traffickers."[78]

One early case, the prosecution of Benjamin Gaston, helped to show the benefits of Memex to DANY.[79] Gaston found a woman advertising sexual services online, kidnapped her, and then forced her to earn money for him by having sex with other men.[80] After two days and numerous sexual assaults, the victim "attempted to escape from the sixth-floor window of the room where she was being held, falling

---

[74] *Id*.

[75] Larry Greenemeier, *Human Traffickers Caught on Hidden Internet*, SCIENTIFIC AMERICAN (Feb. 8, 2015), https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/.

[76] NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE, MANHATTAN DISTRICT ATTORNEY'S OFFICE APPLIES INNOVATIVE TECHNOLOGY TO SCAN THE "DARK WEB" IN THE FIGHT AGAINST HUMAN TRAFFICKING (Feb. 9, 2015), http://manhattanda.org/press-release/manhattan-district-attorney's-office-applies-innovative-technology-scan-"dark-web"-fig.

[77] Graeber, *supra* note 66.

[78] NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE, *supra* note 104.

[79] *Id*.

[80] *Id*.

more than 50 feet to the ground, breaking multiple bones."[81] DANY was able to verify the victim's testimony by conducting Memex searches for advertisements with her photo on the dark web. Utilizing the information from the Memex queries, prosecutors were able to establish a timeline that confirmed the victim's statements and strengthened the case. Gaston later received a sentence of 50-years-to-life in state prison.[82]

The case of Froilan Rosado also highlights the success of Memex in DANY. Law enforcement began investigating Rosado in 2014 after picking up an 18-year-old prostitute in a sting operation. The prostitute told police that she had previously been kicked out of her foster home and had nowhere to go. Rosado had taken her in and then began pimping her out. Rosado, investigators would discover, was an expert at luring girls over social media, some as young as 15. He then used drugs and violence to keep them in the sex trade.[83]

Prosecutors wanted to build a strong case against Rosado, but they did not know the names, phone numbers, or whereabouts of his other victims. This was especially difficult because Rosado frequently changed the online advertisements for the girls he trafficked. He also changed the girls' names and utilized pre-paid, disposable cell phones (i.e. burner phones). All these details made it difficult for investigators to tie Rosado to a larger prostitution ring.[84]

Investigators then utilized the Memex tools Dig and TellFinder to mine information about Rosado's deleted and current sex ads. The search results linked photos, names, emails, phone numbers, and previously unknown victims. Investigators were even able to take new phone numbers mentioned over the phone by Rosado (who was still running his sex trafficking ring while awaiting trial at Rikers Island) and search for even more new connections in Memex. Investigators were eventually able to link Rosado to a prostitution ring of 10 teenagers ranging from 15 to 18 years old. On September 15, 2015, Rosado received a sentence of 7-to-14 years in prison after guilty verdicts for all of the charges against him: one count of Sex Trafficking, and two counts of Promoting Prostitution in the Third Degree.[85]

---

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE, DA VANCE: FROILAN ROSADO SENTENCED TO 7-TO-14 YEARS FOR PROSTITUTING TEENAGE GIRLS (Sep. 15, 2015), http://manhattanda.org/press-release/da-vance-froilan-rosado-sentenced-7-14-years-prostituting-teenage-girls.

Conclusion

The dark web provides a high-degree of anonymity to users, including criminals engaging in illicit activities. In the case of Operation Pacifier, the FBI skillfully gained control of the Playpen server before employing an NIT. This novel approach to identifying individuals who access child pornography on the dark web also raised new challenges from the defense bar. However, the use of NITs to combat criminal behavior on the dark web will likely increase. The revised version of Rule 41 went into effect on December 1, 2016 and will aid law enforcement in obtaining warrants for NITs. State and local investigators may also employ NITs as departments gain the required technical expertise.

Additionally, Memex and other dark web data-mining tools will continue to proliferate within the law enforcement community. These platforms provide powerful ways to sift through large volumes of information and provide links of criminals trafficking humans on the dark web. Traditional law enforcement techniques, such as undercover or surveillance operations, still serve an important part in combatting crime on the dark web. However, increasingly, investigators and prosecutors may need to turn to cutting-edge technology in order to identify suspects, build cases, and prosecute dark web criminals.