ARTICLE:

Network investigative source code and due process

By **Brian L. Owsley**

The federal government has developed an electronic computer tool known as the Network Investigative Technique ('NIT'). Essentially, an NIT is a device used by law enforcement to invade an individual computer to obtain access to and obtain all types of information, including computer files, pictures, emails, and other data.[1] The government has had some success recently targeting large secretive networks of individuals sharing child pornography.[2]

This success has led to numerous prosecutions of those receiving and sharing child pornography. However, in response, defendants are starting to raise challenges to the manner in which this technology functions. The courts are struggling with where to draw the line between a defendant's right to a fair trial, which may be infringed upon if the defendant does not have adequate understanding of how the technology works, and the government's interest in maintaining secrecy regarding the investigative tools that it develops.[3] For example, criminal defence attorneys in Baltimore were largely unaware that officers with the Baltimore Police Department used cell site simulators over 4,000 times in criminal investigations.[4]

This article addresses the use of NITs in the prosecution of a series of related child pornography cases. The first part addresses not only how the FBI began investigating the child pornography distribution ring, but also the issuance of a search warrant by a federal magistrate judge in Virginia that was central to the indictment and prosecution of each defendant around the country. In response to their indictment and prosecution, the defendants raised a number of legal challenges to the FBI's use of the NIT. These various challenges are discussed in the second part. Most defendants did not succeed in avoiding a conviction for some kind of child pornography charge. However, the third part discusses one case that resisted this trend of convictions based on the notion that the defendant needed access to the NIT source code in order properly defend himself.

Factual background

Child pornographers developed a website known as 'Playpen' to enable them to distribute and share child pornography amongst themselves.[5] This website had over 158,000 people who were authorized to obtain access, and each day about 1,500 people viewed child pornography on it.[6]

The FBI gets involved in the investigation of a child pornography distribution network

At the beginning of 2015, the FBI learned that this website was being operated on a United States-based IP address on CentriLogic, a server in Lenoir, North Carolina.[7] In January 2015, the FBI executed a search warrant on CentriLogic and got a copy of the Playpen website.[8] On February 19, 2015, the FBI arrested Steven Chase, the person believed to be operating Playpen.[9] Instead of shutting down the server hosting Playpen, the FBI seized a copy of the server and moved it to a governmental server located in Newington, Virginia where the copy of the server was

[1] See Brian L. Owsley, 'Beware of Government Agents Bearing Trojan Horses,' 48 Akron L. Rev. 315, 315-16 (2015).
[2] The words 'child pornography' are used in this article because it is a term of art that defines the crime.
[3] Defense attorneys not only need to be aware that law enforcement is using new technologies, but how to defend against such usages. *See United States v. Wilford*, No. 11-0258, 2016 WL 759174, at *10 (D.Md. Feb. 26, 2016) (unpublished).
[4] See Brad Heath, 'Police secretly track cellphones to solve routine crimes,' USA Today, (Aug. 23, 2015) available at https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ .
[5] See *United States v. Allain*, 213 F. Supp. 3d 236, 239 (D. Mass. 2016).
[6] *See United States v. Gaver*, No. 3:16-cr-88, 2017 WL 1134814, at *1 (S.D. Ohio Mar. 27, 2017) (unpublished).
[7] See *United States v. Lough*, 221 F. Supp. 3d 770, 772 (N.D. W. Va. 2016); *United States v. Anzalone*, 221 F. Supp. 3d 189, 191 (D. Mass. 2016); *United States v. Allain*, 213 F. Supp. 3d at 239; *United States v. Croghan*, 209 F. Supp. 3d 1080, 1084 (S.D. Iowa 2016); *Acevedo-Lemus*, No. 15-00137, 2016 WL 4208436, at *1 (C.D. Cal. Aug. 8, 2016) (unpublished).
[8] See *United States v. Anzalone*, 221 F. Supp. 3d at 191.
[9] See *United States v. Anzalone*, 221 F. Supp. 3d at 191; *United States v. Darby*, 190 F. Supp. 3d 520, 526 (E.D. Va. 2016).

allowed to continue operating for two more weeks so that the FBI could gather information to identify the various users of the website.[10] The FBI had regular meetings during this time period to determine whether to keep operating the Playpen website.[11]

The Playpen website ran on the 'The Onion Router' or Tor network, which was created to preserve anonymity of those persons obtaining access to the website by masking their IP address[12] from external viewers.[13] In order '[t]o access the Tor network, a user must download an add-on to the user's existing browser or download the Tor browser bundle.'[14] The Tor network is designed to safeguard anonymity in two principle ways. First, a user's communications with a website like Playpen are routed over a series of relay computers around the world.[15] The only IP address that is revealed is the last one, known as an exit node.[16] Second, the Tor network provides anonymity to the hosts of websites like Playpen. Specifically, '[t]he website's IP address is hidden and replaced with a Tor-based address consisting of a series of alphanumeric characters followed by the suffix '.onion.''[17] The FBI was only able to obtain the Playpen website's IP address because the North Carolina server experienced a misconfiguration.[18] 'This glitch offered the FBI a rare opportunity to locate the server, find the administrator, and identity the site's users.'[19]

United States Magistrate Judge Teresa Buchanan issued a search warrant

Because of the protection offered by the Tor network for its users, the FBI had a difficult time identifying the persons obtaining access to the Playpen website, so they obtained a search warrant to use an NIT on the computers obtaining access to Playpen.[20] On February 20, 2015, the FBI obtained an order from a United States District Judge in the United States District Court for the Eastern District of Virginia authorizing it to intercept communications by individuals viewing the Playpen website.[21] That same day, the FBI also obtained a search warrant from United States Magistrate Judge Theresa Buchanan of the Eastern District of Virginia.[22] The NIT enabled the FBI to obtain the IP addresses of the users on the Playpen website, and in turn, the identity of these individual users.[23] Specifically, '[t]he NIT is a series of code that instructed a user's computer to transmit certain information to the FBI after the user logged on to Playpen.'[24]

Numerous criminal defendants were ultimately identified, indicted, arrested, and prosecuted for federal charges of receiving child pornography[25] and possessing child pornography.[26] In turn, the defendants filed several motions to suppress and other challenges to the use of the NIT, with varying degrees of success.

[10] See *United States v. Allain*, 213 F. Supp. 3d at 239; *Croghan*, 209 F. Supp. 3d at 1084; *United States v. Ammons*, 207 F. Supp. 3d 732, 737 (W.D. Ky. 2016); *United States v. Levin*, 186 F. Supp. 3d 26, 30 (D. Mass. 2016); *United States v. Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *2 (N.D. Ala. Apr. 24, 2017); *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *1 (N.D. Cal. Dec. 8, 2016).

[11] See *United States v. Anzalone*, 221 F. Supp. 3d at 193.

[12] 'An 'Internet Protocol number' is '[t]he unique identification of the location of an end-user's computer, the IP address serves as a routing address for email and other data sent to that computer over the internet from other end-users.' *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 407 (2d Cir. 2004). 'Every computer connected to the Internet has a unique Internet Protocol ('IP') address, which are long strings of numbers, such as 64.233.161.147.' *Liberty Media Holdings, LLC v. Letyagin*, 925 F. Supp. 2d 1114, 1116 n.2 (D. Nev. 2013); *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 284 (2005) ('An IP address is the internet equivalent of a telephone number').' Brian L. Owsley, 'Beware of Government Agents Bearing Trojan Horses,' 48 Akron L. Rev. 315, 315-16 (2015) at 317 n.8.

[13] See *United States v. Allain*, 213 F. Supp. 3d at 239; *United States v. Anzalone*, 208 F. Supp. 3d 358, 361 (D. Mass. 2016).

[14] *United States v. Anzalone*, 208 F. Supp. 3d at 361.

[15] See *Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *1; *United States v. Anzalone*, 208 F. Supp. 3d at 361; *United States v. Ammons*, 207 F. Supp. 3d at 736; *Darby*, 190 F. Supp. 3d at 526.

[16] See *Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *1; *United States v. Ammons*, 207 F. Supp. 3d at 736; *United States v. Darby*, 190 F. Supp. 3d at 526.

[17] See *Ammons*, 207 F. Supp. 3d at 736; accord *United States v. Anzalone*, 208 F. Supp. 3d at 361.

[18] See *United States v. Anzalone*, 221 F. Supp. 3d at 191.

[19] See *United States v. Anzalone*, 221 F. Supp. 3d at 191.

[20] See *United States v. Allain*, 213 F. Supp. 3d 236, 239 (D. Mass. 2016).

[21] See *United States v. Levin*, 186 F. Supp. 3d at 30.

[22] See *United States v. Lough*, 221 F. Supp. 3d at 772-73; *United States v. Ammons*, 207 F. Supp. 3d at 737; *Levin*, 186 F. Supp. 3d at 30; *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *1.

[23] See *United States v. Ammons*, 207 F. Supp. 3d at 737; *United States v. Werdene*, 188 F. Supp. 3d 431, 435 (E.D. Pa. 2016).

[24] *United States v. Ammons*, 207 F. Supp. 3d at 737.

[25] 18 U.S.C. §2252A(a)(2).

[26] 18 U.S.C. §2252A(a)(5).

Legal Challenges to the NIT

Many defendants argued that the FBI lacked probable cause to obtain the NIT search warrants. The district courts handling these cases have addressed a number of the defendants' various arguments.

Magistrate Judge Buchanan's warrant lacked sufficient particularity and thus violated the Fourth Amendment

The Fourth Amendment protects people from searches within their homes by requiring a warrant: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'[27] Moreover, the warrant must describe with particularity the property to be seized or the place to be searched.

In these cases, the defendants argued that their names and addresses should be provided along with the target search for a computer in order to satisfy the Fourth Amendment's particularity requirement. The FBI had to obtain a search warrant to implement the NIT because the FBI's 'deployment of the NIT was a Fourth Amendment search.'[28] Consistent with the Fourth Amendment, such a warrant must describe with particularity the place being searched as well as the items being seized.

The affidavit relied upon by Magistrate Judge Buchanan was very detailed, providing specific information about the Playpen website as well as the use of the TOR to allow the various defendants to obtain access to the website in purported anonymity.[29] The particular place was two-fold: the computer server located in Newington, Virginia and then onto the computers that log into the Playpen website.[30] The affidavit 'clearly listed … seven specific items, including the activating computer's 'actual IP address.''[31] In the end, every court to address a challenge by a Playpen website defendant about the warrant issued by Magistrate Judge Buchanan found that the warrant was sufficiently particular.[32]

Magistrate Judge Buchanan erred by issuing the search warrant

A number of defendants asserted that Magistrate Judge Buchanan lacked authority pursuant to the Federal Rules of Criminal Procedure to issue the search warrant. The affidavit reviewed by the magistrate judge in conjunction with 'the warrant specifically requested authority to embed the NIT on any 'activating computer—*wherever located*.''[33] In February 2015, when she issued the search warrant, generally 'a magistrate judge with authority in the district … ha[d] authority to issue a warrant to search for and seize a person or property located within the district.'[34] There were four other bases upon which a magistrate judge could issue a warrant outside the district. First, a magistrate judge may issue search warrants for persons or property outside the district if the target was within the district when the warrant was signed.[35] Second, a magistrate judge may issue a warrant for anywhere if it involves a terrorism investigation.[36] Third, a magistrate judge may issue a warrant for a tracking device in which the target is within the district, but may move out of it.[37] A magistrate judge may issue warrants for targets in American territories, possessions, commonwealths, diplomatic premises, or residences occupied. American diplomatic personnel.[38]

---

[27] U.S. Const. amend. IV.

[28] *United States v. Darby*, 190 F. Supp. 3d at 530; accord *United States v. Ammons*, 207 F. Supp. 3d at 739 (listing numerous cases concluding that the use of an NIT constituted a search pursuant to the Fourth Amendment); see also *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *2; *United States v. Knowles*, 207 F. Supp. 585, 599 (D. S.C. 2016).

[29] See *United States v. Lough*, 221 F. Supp. 3d at 779; *United States v. Matish*, 193 F. Supp. 3d 585, 607-09 (E.D. Va. 2016).

[30] See *United States v. Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *11.

[31] *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *2; *United States v. Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *11.

[32] *United States v. Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *11 (citing *United States v. Anzalone*, 208 F. Supp. 3d at 368; *United States v. Jean*, 207 F. Supp. 3d 920, 935-36 (W.D. Ark. 2016); *Knowles*, 207 F. Supp. at 602; *United States v. Duncan*, No:3:15-cr-00414, 2016 WL 7131475, at *3 (D. Ore. Dec. 6, 2016) (unpublished); *see also Darby*, 190 F. Supp. 3d at 530 (search warranted was supported by probable cause); *United States v. Michaud*, No.3:15-cr-05351, 2016 WL 337263, at *5 (W.D. Wash. Jan. 28, 2016) (unpublished) ('Both the particularity and breadth of the NIT warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant.').

[33] *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *3.

[34] Fed. R. Crim P. 41(b)(1) (2015).

[35] Fed. R. Crim P. 41(b)(2) (2015).

[36] Fed. R. Crim P. 41(b)(3) (2015).

[37] Fed. R. Crim P. 41(b)(4) (2015).

[38] Fed. R. Crim P. 41(b)(5) (2015).

In April 2016, a new subsection was proposed for 41(b) that became effective December 1, 2016:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> > (A) the district where the media or information is located has been concealed through technological means; or
> >
> > (B) in an investigation of a violation of 18 U.S.C. §1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[39]

However, this new subsection was not available when Judge Buchanan issued her NIT warrant. Consequently, most courts have concluded that the NIT warrant was issue without legal authority.[40]

A few courts have upheld Judge Buchanan's issuance of the warrant pursuant to Rule 41(b)(4), however some of those decisions were from courts that were also in the Eastern District of Virginia, like Judge Buchanan.[41] In *Jean*,[42] Judge Brooks of the Western District of Arkansas determined 'that the FBI's NIT was an electronic tool or technique designed for the purpose of tracking the movement of information both within and outside the Eastern District of Virginia.' The *Jean* court concluded that Judge Buchanan had the authority to issue the NIT warrant pursuant to Rule 41(b)(4).[43] A few other decisions from outside the Eastern District of Virginia also concluded that the NIT warrant was valid pursuant to Rule 41(b)(4).[44]

At least one district court explicitly rejected *Jean* and its conclusion that the NIT warrant operated as a tracking device.[45] In *Croghan*,[46] the court concluded that the NIT 'clearly did not 'track' the 'movement of a person or object.'' Instead 'it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia.'[47] Nonetheless, most courts have rejected the idea that this violation of Rule 41 constituted prejudice to the Playpen defendants.[48]

Reasonable expectation of privacy in the use of IP addresses

Some defendants argued that they had a reasonable expectation of privacy in their IP addresses. The Supreme Court first enunciated the reasonable expectation of privacy standard in *Katz v. United States*,[49] in Justice Harlan's concurring opinion. That analysis is often weakened by the Supreme Court's development of the 'third party doctrine'.[50] In *Smith*, the Court held that the defendant did not have any expectation of privacy in the numbers that he dialled on his telephone because he conveyed those telephone numbers to the telephone company—a third party—in order to complete the telephone call.[51]

[39] Fed. R. Crim P. 41(b)(6) (2016).
[40] For example, see *United States v. Croghan*, 209 F. Supp. 3d at 1086-89; *United States v. Ammons*, 207 F. Supp. 3d at 740-41; *Knowles*, 207 F. Supp. at 599-600; *Werdene*, 188 F. Supp. 3d at 440-42; *United States v. Levin*, 186 F. Supp. 3d 26, 32-34 (D. Mass. 2016); *Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *3; *United States v. Henderson*, No. 15-cr-00565, 2016 WL 4549108, at *3 (Sept. 1, 2016) (unpublished); *United States v. Michaud*, 2016 WL 337263, at *6; *United States v. Gaver*, 2017 WL 1134814, at *8-9; see also *Taylor*, _ F. Supp. 3d _, 2017 WL 1437511, at *12 (declaring that the warrant was void ab initio); *United States v. Levin*, 186 F. Supp. 3d at 35 (same).
[41] See *United States v. Matish*, 193 F. Supp. 3d at 612-13; *Darby*, 190 F. Supp. 3d at 536; *United States v. McLamb*, _ F. Supp. 3d _, 2016 WL 6963046, at *6 (E.D. Va. Nov. 28, 2016); *United States v. Eure*, No. 2:16cr43, 2016 WL 4059663, at *4 (E.D. Va. July 28, 2016) (relying on the analysis in *Darby*).
[42] *United States v. Jean*, 207 F. Supp. 3d at 937-38.
[43] See *United States v. Jean*, 207 F. Supp. 3d at 938; see also *United States v. Austin*, _ F. Supp. 3d _, 2017 WL 496374, at *4-5 (M.D. Tenn. Feb. 2, 2017) (adopting the reasoning and the analysis of *Jean*).
[44] *United States v. Austin*, _ F. Supp. 3d _, 2017 WL 496374, at *4-5 (analogizing NIT to tracking device); *United States v. Sullivan*, _ F. Supp. 3d _, 2017 WL 201332, at *5 (N.D. Ohio Jan. 18, 2017) (same).
[45] See *United States v. Croghan*, 209 F. Supp. 3d at 1087-89.
[46] *United States v. Croghan*, 209 F. Supp. 3d at 1088; see also *United States v. Adams*, No. 6:16-cr-11, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) ('the NIT does not track; it searches').
[47] *United States v. Croghan*, 209 F. Supp. 3d at 1088.
[48] See *United States v. Werdene*, 188 F. Supp. 3d at 446-47; *United States v. Michaud*, 2016 WL 337263, at *6-7; *United States v. Epich*, No 15-cr-163, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) (unpublished).
[49] 389 U.S. 347 (1967).
[50] See generally *Smith v. Maryland*, 442 U.S. 735 (1979), see also *United States v. Miller*, 425 U.S. 435 (1976).
[51] See 442 U.S. at 742-43.

Some courts have determined that defendants do not have an expectation of privacy in their IP addresses.[52] However, other courts viewed it differently in that the defendants have a reasonable expectation of privacy in the use of their computers that should preclude the issuing of a warrant.[53] In *Ammons*,[54] the court rejected the government's argument that the third party doctrine applied to the defendant's IP address, noting that 'the Government obtained Ammons' IP address from a search of his personal computer—not, for example, from a third party provider.' Similarly, the *Darby*[55] court rejected the government's third party doctrine argument explaining that the important question was whether the defendant had an expectation of privacy in the use of his computer, especially in light of the fact that '[t]he NIT surreptitiously placed code on Defendant's personal computer that then extracted from the computer certain information.'

Whether the FBI violated of due process by operating the website

A few defendants argued that the federal government's operation of the Playpen website for a couple of weeks was outrageous and in violation of due process.[56] Indeed, the Supreme Court has determined dismissal of criminal charges against a defendant is permissible in those cases when law enforcement's misconduct violates 'fundamental fairness, shocking to the universal sense of justice,' as mandated by the Due Process Clause of the Fifth Amendment.'[57]

In *Anzalone*,[58] the defendant argued 'that the number of visitors to Playpen increased significantly during the two weeks the government ran the site.' However, the district court determined 'that the number of visitors did not appreciably increase when the government began operating the site.'[59] In addition to this argument, the defendant also maintained that the FBI could have blocked access to the site containing illegal images, and that it failed to make any attempt to control the distribution of the images during this two-week period.[60] Ultimately, the court in *Anzalone* ruled that the FBI's operation of the Playpen website did not violate the due process clause.[61] Similarly, in *Allain*,[62] although the district court acknowledged discomfort with the FBI's role in facilitating access to child pornography for the two weeks that it operated the Playpen website, it ultimately concluded that the FBI did not act in an outrageous manner, especially in light of the difficulty to investigate and charge crimes such as the distribution of child pornography.

The courts generally declined to apply the exclusionary rule

Almost all courts concluded that the evidence obtained pursuant to the NIT warrant should be admitted in the prosecution of the various defendants. In other words, even if the extraction of information from the defendants' computers violated the Fourth Amendment, the courts did not suppress the evidence.

Typically, the courts would find that the good faith exception to the exclusionary rule applied.[63] In *United States v. Leon*,[64] the police obtained information that Patsy Stewart and Armando Sanchez were selling drugs.[65] Consequently, police officers began monitoring the homes of both Sanchez and Stewart.[66] Based on this monitoring, they learned that Alberto Leon and Ricardo Del Castillo were selling drugs with Sanchez and Stewart.[67] The police obtained a warrant based on information that they observed as well as information from an informant.[68] After the search, it was determined that the police lacked probable cause.[69] Furthermore, the trial court rejected the government's request that the evidence obtained from this invalid search be admitted because the

[52] See *United States v. Werdene*, 188 F. Supp. 3d at 443-45; *United States v. Acevedo-Lemus*, 2016 WL 4208436, at *6; *United States v. Lough*, 221 F. Supp. 3d at 774-76.
[53] See *United States v. Ammons*, 207 F. Supp. 3d at 739; *United States v. Darby*, 190 F. Supp. 3d at 528-29.
[54] See *United States v. Ammons*, 207 F. Supp. 3d at 739 (citing *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016)).
[55] *United States v. Darby*, 190 F. Supp. 3d at 529.
[56] See *United States v. Anzalone*, 221 F. Supp. 3d at 193-95; *United States v. Allain*, 213 F. Supp. 3d at 252-53.
[57] *United States v. Russell*, 411 U.S. 423, 432 (1973) (quoting *Kinsella v. United States ex rel. Singleton*, 361 U.S. 234, 246 (1960)).
[58] *United States v. Anzalone*, 221 F. Supp. 3d at 192.
[59] *United States v. Anzalone*, 221 F. Supp. 3d at 193.
[60] See *United States v. Anzalone*, 221 F. Supp. 3d at 194.
[61] See *United States v. Anzalone*, 221 F. Supp. 3d at 195.
[62] See *United States v. Allain*, 213 F. Supp. 3d at 253.
[63] *United States v. Darby*, 190 F. Supp. 3d at 529.
[64] 468 U.S. 897 (1984).
[65] See 468 U.S. 897 (1984) at 901.
[66] See 468 U.S. 897 (1984) at 901.
[67] See 468 U.S. 897 (1984) at 901.
[68] See 468 U.S. 897 (1984) at 901-02.
[69] See 468 U.S. 897 (1984) at 903.

police relied on the warrant that they received and acted in good faith on it.[70]

In *Leon*,[71] the Supreme Court concluded that evidence obtained based on an invalid search warrant could be admitted. It explained that the exclusionary rule is just a remedy designed to prevent illegal police action. Here, the exclusionary rule's costs outweigh its benefits because otherwise guilty people would not be convicted. On the other hand, it would not prevent bad police behaviour, and the police will not change some improper behaviour when they are relying in good faith on a warrant from a judge. Specifically, it explained that '[w]hen police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant.[72]

The Supreme Court fashioned the exclusionary rule to prevent the admission of improperly obtained evidence. However, the Court has further elaborated by explaining that the exclusion of evidence is not 'an automatic consequence of a Fourth Amendment violation.[73] Instead, courts must analyze whether 'the deterrence benefits of suppression … outweigh its heavy costs.'[74]

Most of the courts analyzing the error by Magistrate Judge Buchanan concluded that the defendants did not suffer any prejudice, and thus, the exclusionary rule should not apply. For example, a district judge could have issued the same warrant without any jurisdictional issues like the ones that most courts found regarding the NIT warrant.[75] Even when courts have determined that the NIT warrant was void from the beginning, some have still determined that the good faith exception applied.[76]

The due process clause provided a child pornography defendant with an argument for access to the source code

As will be observed, most defendants in these Playpen cases did not succeed in avoiding conviction notwithstanding legitimate concerns about the FBI's investigative methods, including its use of the NIT. This will not be an issue in the future because Rule 41 has recently been amended and specifically addresses such concerns and would clearly authorize similar warrants in the future.

The next section explores a case in which the defendant although charged was not convicted for child pornography in a Playpen case. The decision to dismiss the charge is consistent with Supreme Court precedent and similar to successful results some criminal defendants had in challenging prosecution for driving while intoxicated by seeking source code relate to the operation of a breathalyzer.

United States v. Michaud

There is a due process issue that was not raised by many defendants that could have great significance. United States District Judge Robert Bryan from the Western District of Washington discussed the tension between a defendant's right to a fair trial, including the source code information for the FBI's NIT, against the government's interest in maintaining its proprietary information:

> The resolution of Defendant's Third Motion to Compel Discovery places this matter in an unusual position: the defendant has the right to review the full N.I.T. code, but the government does not have to produce it. Thus, we reach the question of sanctions: What should be done about it when, under these facts, the defense has a justifiable need for information in the hands of the government, but the government has a

[70] See 468 U.S. 897 (1984) at 904.
[71] See 468 U.S. 897 (1984) at 916.
[72] 468 U.S. 897 (1984) at 922; accord *Herring v. United States*, 555 U.S. 135, 142 (2009) (quoting *Leon*).
[73] *United States v. Herring*, 555 U.S. 135 at 137.
[74] *Davis v. United States*, 564 U.S. 229, 237 (2011) (citing *Herring*, 555 U.S. at 141).
[75] See *United States v. Matish*, 193 F. Supp. 3d at 622-23; *Darby*, 190 F. Supp. 3d at 538-39; *United States v. Werdene*, 188 F. Supp. 3d at 450-53; *United States v. Levin*, 186 F. Supp. 3d at 43-44; *United States v. Hammond*, _ F. Supp. 3d _, 2016 WL 7157762, at *5 (discussing *Levin*); *United States v. Ammons*, 207 F. Supp. 3d at 744; *United States v. Henderson*, 2016 WL 4549108, at *6; *United States v. Adams*, 2016 WL 4212079, at *7-8; *United States v. Acevedo-Lemus*, 2016 WL 4208436, at *8; *United States v. Michaud*, 2016 WL 337263, at *7.
[76] *United States v. Ammons*, 207 F. Supp. 3d at 739; *United States v. Werdene*, 188 F. Supp. 3d at 447-51; *United States v. Eure*, 2016 WL 4059663, at *8.

> justifiable right to turn the information over to the defense?[77]

In addressing these questions, the district judge determined that the evidence withheld by the government regarding the source code was central to the defence.[78] Moreover, if the government were allowed to introduce evidence without the defendant having a meaningful response based on the lack of access to the source code, the weight of the evidence obtained from the NIT would be prejudicial.[79]

Consequently, because 'the discovery withheld implicates the defendant's constitutional rights,' the district judge determined 'that the evidence of the NIT and the search warrant issued on the basis of the NIT should be suppressed, and the fruits of that search must also be suppressed.'[80] In turn, the government concluded that, without that evidence, it could not establish the defendant's guilt beyond a reasonable doubt so it moved to dismiss the indictment without prejudice.[81] The court subsequently granted the motion to dismiss.[82] In other words, the government's prosecution of Michaud came to a halt when it chose to keep the source code secret instead of providing it consistent with the court order.

Jencks v. United States

In *Jencks v. United States*,[83] the Supreme Court considered the case of Clinton Jencks who was being prosecuted for filing a false ''Affidavit of Non-Communist Union Officer' with the National Labor Relations Board.'[84] During the criminal trial, the government called two witnesses who were members of the Communist Party providing information to the FBI about party activities.[85] These two individuals prepared written reports for the FBI, which the criminal defence sought in order to utilize during cross-examination, but the district judge denied these motions to produce.[86]

The Court explained that '[r]elevancy and materiality for the purposes of production and inspection, with a view to use on cross-examination, are established when the reports are shown to relate to the witness.'[87] The Court had previously determined that the government's prosecutorial role also involves the need to promote justice that it would be inappropriate for the prosecution 'to its governmental privileges to deprive the accused of anything which might be material to his defense.'[88] Ultimately, the *Jencks* Court held that when the government asserts its privilege and refuses to produce documents in violation of a court order, the criminal prosecution must be dismissed.[89]

Minnesota criminal defendants have successfully attacked driving while intoxicated prosecutions by seeking the breathalyzer source codes

Many individuals have argued in state courts for production of breathalyzer source code so that they can defend themselves against charges of driving while intoxicated. Some courts have granted such requests pursuant to due process concerns. In Minnesota, a defendant may be entitled to disclosure of a breathalyzer's source code if the defendant can establish that such information is relevant to the defendant's guilt or innocence.[90] For example, in *Lund v. Commissioner of Public Safety*,[91] the Court of Appeals of Minnesota determined that it was reversible error for the trial court to deny a person defending an action to revoke his driver's license access to the breathalyzer source code.[92] In reversing the trial court's decision to deny a request for the source code, the appellate court noted that 'Lund submitted an expert affidavit explaining the relevancy

[77] Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, *United States v. Michaud*, No.3:15-cr-05351 (W.D. Wash. May 18, 2016).
[78] Transcript at 19, *United States v. Michaud*, No.3:15-cr-05351 (W.D. Wash. May 25, 2016) filed with the clerk on July 26, 2016.
[79] *United States v. Michaud* at 20.
[80] *United States v. Michaud* at 21-22.
[81] Government's Unopposed Motion to Dismiss Indictment Without Prejudice, *United States v. Michaud*, No.3:15-cr-05351 (W.D. Wash. Mar. 3, 2017).
[82] Order Dismissing the Indictment Without Prejudice, *United States v. Michaud*, No.3:15-cr-05351 (W.D. Wash. Mar. 6, 2017).
[83] 353 U.S. 657 (1957).
[84] 353 U.S. 657 (1957) at 658.
[85] 353 U.S. 657 (1957) at 659.
[86] 353 U.S. 657 (1957).
[87] 353 U.S. 657 (1957) at 669.
[88] *United States v. Reynolds*, 345 U.S. 1, 12 (1953); accord *Jencks*, 353 at 671.
[89] See *Jencks*, 353 at 672 (citing *Roviaro v. United States*, 353 U.S. 53, 60-61 (1957)).
[90] See generally *State v. Underdahl*, 749 N.W.2d 117 (Minn. Ct. App. 2008).
[91] No. A08-1408, 2009 WL 1587135 (Minn. Ct. App. June 9, 2009) (unpublished).
[92] No. A08-1408, 2009 WL 1587135 (Minn. Ct. App. June 9, 2009) (unpublished) at *3.

of the source code to his defense.'[93] On this basis, the court declined to address the due process issue.[94] Similarly, in *State v. Kummer*,[95] the appellate court addressed the prosecution's interlocutory appeal of a trial court decision that ordered the state to provide the defendant with the breathalyzer's source code.[96] Although the prosecution was concerned that the trial court would dismiss its prosecution of Kummer if it refused to provide the source code, the appellate court dismissed the appeal because the prosecution did not establish a jurisdictional basis for its interlocutory appeal.[97]

However, if a defendant failed to establish that the source code was relevant to its defence in demonstrating innocence or negating guilt, the Minnesota courts have denied defendants' request for the breathalyzer source code.[98] Moreover, defendants often waived their right to assert due process challenges related to the breathalyzer source codes by failing to assert them before the trial court.[99] Indeed, the demand for access to the breathalyzer's source code grew frequent enough that the State of Minnesota brought a civil action against the manufacturer of the breathalyzer that its law enforcement agencies regularly used.[100]

Conclusion

The Minnesota cases do not rely on the due process clause in the same manner as *Michaud* did. However, they demonstrate the importance that is enshrined in *Jencks* for criminal defendants to be able to have access to information to put on a defence. As source code becomes more ubiquitous, defendants and their defence attorneys will call for their production.

The Playpen website criminal prosecutions demonstrate the importance of NITs to federal law enforcement agencies. However, there were prosecutions involving these devices prior to the FBI's investigation of the Playpen website.[101] Moreover, the FBI has used these devices to investigate crimes other than child pornography, including terroristic threats, bank fraud, and identity theft.[102] In other words, this is an investigative tool that the government is quite likely to use more frequently in the future as circumstances warrant to obtain information on personal computers and other electronic devices. As this usage grows, so will the likely challenge by criminal defendants seeking the source code.

Brian L. Owsley, Assistant Professor of Law, University of North Texas Dallas College of Law; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs. The author previously served as a federal magistrate judge in the United States District Court for the Southern District of Texas.

[93] No. A08-1408, 2009 WL 1587135 (Minn. Ct. App. June 9, 2009) (unpublished) at *3.
[94] See No. A08-1408, 2009 WL 1587135 (Minn. Ct. App. June 9, 2009) (unpublished) at *3; see also *State v. Bunker*, No. A08-2191, 2009 WL 1752564, at *3 (Minn. Ct. App. June 23, 2009) (unpublished) ('It is unnecessary to address the state's argument regarding respondent's due-process rights, because we have determined that the district court did not abuse its discretion in ordering production of the source code.').
[95] No. A08-0533, 2008 WL 4472610 (Minn. Ct. App. Oct. 7, 2008) (unpublished).
[96] No. A08-0533, 2008 WL 4472610 (Minn. Ct. App. Oct. 7, 2008) (unpublished) at *1.
[97] No. A08-0533, 2008 WL 4472610 (Minn. Ct. App. Oct. 7, 2008) (unpublished) at *2; see also *Bunker*, 2009 WL 1752564, at *3 (affirming the trial court's decision to compel production of the breathalyzer's source code to defendant).
[98] See *State v. Garberg*, No. A09-914, 2010 WL 772622, at * 3 (Minn. Ct. App. Mar. 9, 2010) (unpublished).
[99] See *Christian v. Comm'r of Pub. Safety*, No. A13-1921, 2014 WL 1758374 (Minn. Ct. App. May 5, 2014) (unpublished); see also *State v. Sterling*, 782 N.W.2d 579, 581 n.2 (Minn. Ct. App. 2010) (holding that defendant lacked standing to assert that he was denied due process because he did not receive the breathalyzer source code, when those results were not used to convict him for DWI).
[100] See *State of Minnesota ex rel. Campion v. CMI of Ky, Inc.*, No. 08-603, 2009 WL 2170134 (D. Minn. July 16, 2009) (unpublished); see also Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017) ¶ 6.184. http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence
[101] See *generally United States v. Huyck*, 849 F.3d 432 (8th Cir. 2017).
[102] See Brian L. Owsley, 'Beware of Government Agents Bearing Trojan Horses,' 48 Akron L. Rev. 315, 315-16 (2015) at 324-40.