DARKNETS ON THE EDGE OF TOWN: SUPPRESSING EVIDENCE IN THE NEW AGE OF CHILD PORNOGRAPHY PROSECUTIONS

Everybody's got a secret, Sonny,
Something that they just can't face,
Some folks spend their whole lives trying to keep it,
They carry it with them every step that they take.
Till some day they just cut it loose
Cut it loose or let it drag 'em down,
Where no one asks any questions,
or looks too long in your face,
In the darkness on the edge of town.

Stanza 2, Darkness on the Edge of Town,
Bruce Springsteen and the E Street Band

Michael J. Iacopino
Brennan Lenehan
85 Brook Street
Manchester NH 03104
miacopino@brennanlenehan.com

I. Changing Investigative Techniques

Historically, the typical defendant charged with possession or receipt of child pornography is discovered, investigated, arrested and prosecuted as the result of online activity. Typical scenarios include the sharing of child pornography images with undercover officers posing as a teenager or younger child; the receipt and/or transfer of child pornography through peer-to-peer networks; the receipt or transfer of child pornography via e-mail; the receipt or purchase of child pornography on the World Wide Web using familiar internet browsers such as Internet Explorer or Safari.

Today computer users are capable of accessing secret parts of the internet. Often called the Dark Net or Dark Web there are portions of the internet where web sites can hide their locations through numerous routing layers that can only be reached through the use of the Tor web browser which maintains the anonymity of the network. The Tor network directs web traffic across several different servers or "relays" and encrypts the traffic by hiding public IP addresses through non-traceable routing. Tor network servers identify an IP address from a Tor exit relay, which can be anywhere in the world and therefore anonymous. The Dark Net or Tor network reportedly contains all sorts of access to illegality including mail order drugs and child pornography.

Over the years law enforcement has dedicated more resources to investigation child pornography and has developed techniques that when successfully applied may result in the arrests of hundred if not thousands of individuals. In recent years the Government has focused its effort on the Dark Web. In cases where the Government has been able to identify and take over a Tor based child pornography server it has developed Network Investigative Techniques (NITs.) The NITs currently used by the Government allow investigators to essentially hack the computer of anyone who visits the government controlled web site. The use of NITs is sometimes referred to as drive-by hacking.

A brief comparison of old methods and new:

A. The Old Order – Operation Emissary

From early October, 2005 through 2008 U.S. Immigration and Customs enforcement (ICE) conducted a three phase investigation entitled Operation Emissary, Emissary II and Thin Ice. The first phase of the investigation began when ICE agents identified a child pornography website available on the internet titled "Illegal.CP." Undercover agents joined the website by paying $79.99 for a twenty day membership and then accessed various web pages containing thousands of child pornography images. The agents determined that the images were housed on a server in Orlando, Florida. The agents conducted searches of the Orlando server in mid-November, 2005, December 2005 and January 2006. The three searches of the Orlando server revealed thousands of child pornography images and log files identifying hundreds of IP addresses for users of the various web pages. The agents later learned that the server had been transferred to McLean Virginia in December 2005. Searches of the McLean server were conducted in February and March of 2006. Upon discovering hundreds of IP addresses the agents used administrative subpoenas to identify the internet service providers and the owners of the IP addresses that had accessed the websites. Search warrants were obtained and approximately 250 people were arrested and convicted as a result of the first phase of the investigation.

The second phase of the investigation began in February 2006 and focused on obtaining information from the credit card processing company employed by the owners of the child pornography web site. In September 2006 a search warrant executed at the credit card processing company revealed a database identifying, by credit card information, numerous customers of the child pornography website. The second phase of the investigation led to the arrests and convictions of hundreds more.

Phase three of the investigation began in March 2006 when ICE enlisted a confidential witness who had been involved in the credit card processing for the child pornography website. The CW had been arrested and charged with money laundering. The CW assisted the agents by convincing the operators of the web sites to use a CW controlled merchant account to process credit card transactions. ICE agents took control of the merchant account. All of the transactions were then obtained by the agents who were actually controlling the merchant account. The owners of the web site would then be supplied with information as to which transaction processed and would allow the purchaser to access the child pornography site. Interestingly in this phase of the investigation the agents actually assisted in the purchase and sale of the access to the child pornography. The third phase of the investigation resulted in many more arrests and two more searches of a third server in Tampa, Florida, in the summer of 2008. Ultimately the owner of the child pornography website was located and arrested in the Ukraine.

Notably, many users of the website obtained access to thousands of images of child pornography while the agents controlled and facilitated the credit card processing that allowed access to the child pornography.

The three phases of the Operation Emissary resulted in the conviction of 600 people in 47 states. Although the investigation involved computers, the investigative techniques used were traditional: search warrants for specific places and subpoenas for specific things such as IP addresses.

B. The New World – The Playpen Cases

The rise of the Dark Net has made the old school investigation of child pornography obsolete because in the Dark Net or Tor Network IP addresses (which are normally public and traceable on the WWW) are no longer identifiable because the IP address that is seen by the host website is the IP address of the last exit node relay and not the IP address actually assigned to the website user's computer.

While not the first use of a NIT by government agencies the Playpen Cases represent the most recent. In February 15, 2015, law enforcement agents seized a computer server in North Carolina. That computer allegedly served one of the largest child pornography sites in the world. Rather than immediately shutting down the Playpen site, the FBI developed a NIT that would allow the hijacked computer to search every computer that contacted the network. The hijacked server through the NIT would then extract (ie seize) identifying information which would be transmitted to a government computer and would ultimately allow identification of the owner.

The general operation of NIT's method has been described in search warrant affidavits as follows: Between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into the Playpen website by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would identify the computer, its location, other information about the computer, and the user of the computer accessing the Playpen website. That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

The FBI obtained approximately 1300 IP addresses (and corresponding additional information) over the two week period that the FBI was serving up child pornography to the Dark Net. Remarkably all 1300 searches undertaken by the NIT were conducted pursuant to one search warrant issued by a magistrate judge in the Eastern District of Virginia.

II. Motions to Suppress in Playpen Cases

The issuance of a single search warrant that authorized the intrusion into 1300 homes and the seizure of information stored on a home computer is likely to generate a constitutional debate. Surprisingly that debate, at least to date, has not centered on whether such a warrant is a general warrant of the type abhorred by the Founders. Instead the crux of the debate has centered on the authority of a magistrate judge to issue an extra-jurisdictional warrant under the Federal Magistrate Act, 28 U.S.C. § 636(a) and F.R.Cr.P. 41.

As Playpen cases are litigated in federal courts across the country the most trodden battleground is litigation over the authority of a United States Magistrate Judge to issue an extraterritorial search warrant. For the most part, the District Courts that have considered the issue have found that the Playpen magistrate judge did not have authority to issue the warrant under the Federal Magistrate Act, 28 U.S.C. § 636(a)which encompasses F.R.Cr.P. 41. *See United States v. Croghan*, No. 15-cr-48 (S.D. Iowa Sept. 19, 2016), *United States v. Levin,* No. 15-cr-10271-WGY, (D.MA. May 5, 2016), *United States v. Arterbury,* No. 15-cr-182-JHP (N.D.Okl. Apr. 25, 2016). However, several of the cases that have a Rule 41 violation but have found that the good faith exception to the warrant clause applies. *See United States v. Torres,* No. 16-cr-285-DAE (W.D.Tex. Sept. 9, 2016), *United States v. Adams*, No. 16-cr-11-ORL (M.D. Fla. Aug. 10, 2016), *United States v. Werdene*, No 15-cr-434 (E.D. Pa. May 18, 2016), *United States v. Michaud,* No. 15-cr-05351-RJB (W.D. Wash. January 28, 2016). Three District Courts have found authority for the magistrate to issue the warrant. *See United States v. Jean,* No. 15-cr-50087-001 (W.D. Ark. Sept. 13, 2016), *United States v. Acevedo-Lemos,* No. 15-cr-00137-CJC (C.D. Calif. Aug. 8, 2016), *United States v. Matish,* No. 16-cr-16 (E.D. Vg. Jun. 23, 2016), *United States v. Darby,* No. 16-cr-36 (E.D. Vg. Jun. 3, 2016); *See also United States v. Eure,* No. 16-cr-43 (E.D. Vg., Jul. 28, 2016)(District Judge relies on his previous ruling in *Darby*.)

A. Successful Suppression of Evidence Obtained Via a NIT Warrant

1. Maintain the Constitutional Nature of the Violation

In seeking suppression of evidence obtained via a NIT warrant criminal defense lawyers will want to liberally cite to the opinions written by Judge Wolf in *Levin* and Judge Pratt in *Coghan.* At the outset in *Levin*, Judge Wolf is careful to note that the real issue in contention is "the magistrate judge who issued the NIT Warrant had no authority to do so under the relevant statutory framework and federal rules – not that the issuance of the warrant "violated" these provisions, by, for example, failing to comply with procedural requirements." *United States v. Levin,* No. 15-cr-10271-WGY, slip op. at p. 7 (Fn. 7) (D.MA. May 5, 2016). Defense counsel should maintain a strong stance in motions and in any oral argument that the issue in dispute:

> cannot be considered merely ministerial or procedural because the Rule "involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant." (citing United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008) (holding that Rule 41(b) "deals with substantive judicial authority-not procedure") and Krueger, 809 F.3d at 1115 n.7 (concluding that Rule 41(b)(1) is "unique from other provisions of Rule 41because it implicates 'substantive judicial authority'")). Stated another way,

> because "the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval" of the NIT Warrant as required by the Fourth Amendment.

United States v. Croghan, No. 15-cr-48, slip op. p. 7 (S.D. Iowa Sept. 19, 2016) *quoting Levin* at slip op. p. 17. Maintaining that the issue is a substantial constitutional issue will appropriately frame the issue and will also assist defense counsel in opposing arguments based on good faith.

2. The Federal Magistrate Act and F.R.Cr.P. 41 Are Intertwined and Neither Authorize a Magistrate Judge to Issue an Extraterritorial NIT Warrant

The courts ordering suppression note that the Federal Magistrate Act, 28 U.S.C. § 636(a) and F.R.Cr.P. are intertwined. Citing to *United States v. Krueger*, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring) *Levin* recognizes that the Federal Magistrate Act provides "jurisdictional limitations on the power of magistrate judges." The Federal Magistrate Act, in pertinent part, confines a magistrate judge's within her judicial district and to "all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure [.]" *See* 28 U.S.C. § 636(a)(1)

F.R.Cr. P. 41(b), in relevant part, identifies the authority of a magistrate judge to issue a search warrant:

> At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may

> authorize use of the device to track the movement of a person or property located within the district, outside the district, or both;

In *Levin* the Government argued that the referenced sections of Rule 41(b) should be interpreted liberally and that the warrant was valid under each section because the computer containing the Playpen website was located in the Eastern District of Virginia. *See Levin* at slip op. p. 11-12. The government's argument focused on the location of the seized Playpen computer. The Government claimed that the search actually occurred in the Eastern District of Virginia because the NIT was obtained from the Eastern District of Virginia computer prior to extracting information from Mr. Levin's computer in the District of Massachusetts. Judge Wolf recognized that the place of the search was actually in the District of Massachusetts. The warrant itself identified the search to be conducted on activating computers. The activating computer in this case was located outside of the Eastern District of Virginia. The court called the government's argument "nothing but a strained, after-the-fact rationalization." *Levin,* slip op. p. 12.

The Levin court also dismissed the Government's generic argument that Rule 41 (B) (one) should be interpreted to allow a search warrant to be issued by a judicial officer in the district with strongest known connection to the search. Judge Wolf recognized this as an attempt by the government to encourage the court to change the words of the statute. *See Levin,* slip opinion at p. 13.

Interestingly, in the *Croghan* case, Judge Pratt indicated that the government had essentially conceded that neither Rule 41 (b) (1) nor Rule 41 (b) (2) provided authority for the issuance of the NIT warrant by a magistrate judge. *Croghan* at slip op. p. 4.

3. The NIT Was Not a Tracking Device

The cases which have upheld the authority of the magistrate judge to issue a new warrant have primarily relied upon Rule 41 (B) (4) and found that the net warrant is analogous to a tracking device. *See United States v. Darby*, No. 16-cr-36, slip op. at p. 13 (E.D. Vg. Jun. 3, 2016); *United States v. Matish*, No. 16-cr-16 (E.D. Vg. Jun. 23, 2016). Judge Pratt rejected the reasoning in *Darby* and *Matish* by reviewing the definition of the term “track”:

> A "tracking device" is defined for purposes of Rule 41 as any "electronic or mechanical device which permits the tracking of the movement of a person or object." See Rule 41(a)(2)(E) (employing the definition of "tracking device" as set out in 18 U.S.C. § 3117(b)). Although the term "track" is not further defined, its ordinary meaning is "[t]o follow up the track or footsteps of; to trace the course or movements of; to pursue by or as by the track left." See http://www.oed.com (last visited Sept. 19, 2016). The NIT here at issue, however, clearly did not "track" the "movement of a person or object." Indeed, it did not "track" the "movement" of anything; rather, 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. Thus, the plain language of Rule 41 and the statutory definition of "tracking device" do not, in this Court's opinion, support so broad a reading as to encompass the mechanism of the NIT used in this case. See Torres, 2016 U.S. Dist. LEXIS 122086, 2016 WL 4821223, at *6 (holding that it "is inappropriate for this Court to engage in a process of finesse justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of [Rule 41(b)] as now written does not provide jurisdiction under these circumstances").

Croghan at slip op. p. 6. Defense counsel in drafting her motion to suppress in cases like this should undertake to identify every way in which the NIT is different than the traditional tracking device. A good start is to note that the “activating computer” is normally within the defendant’s home, the place where he has the greatest expectation of privacy. In addition a traditional tracking device might indicate the where the defendant or his property may be. In this case the NIT does more than that. The NIT intrudes into the Defendant’s computer which can be analogized to a closed container and removes information from that container and send it back to the investigators. This intrusion is substantially more of an invasion of privacy than simply identifying where the defendant or his property may be.

B. Suppression is the Appropriate Remedy

Most of the courts that have denied motions to suppress the NIT evidence have done so after finding that the issuance of the NIT warrant violated Rule 41(b) but that the violation was not constitutional in nature. As mentioned above defense counsel at all times should reiterate that the issuance of the NIT warrant was a constitutional violation because it is the equivalent of a search inside a home with no warrant at all.

1. The Issuance of the NIT Warrant Was Void "Ab Initio" and Good Faith Cannot Rescue the NIT Warrant

Levin and *Croghan* both find that the NIT warrant was issued without judicial authority and is therefore "akin to no warrant at all." *Levi*, slip op. at p. 30; *Croghan*, slip op. at p. 8. Under these circumstances the good faith of the Government cannot rescue the NIT warrant. In coming to his conclusion Judge Wolf determined that the good-faith exception cannot apply to circumstances in which a warrant is void ab initio. After recognizing the question to be one of first impression in the First Circuit, Judge Wolf analyzes United States v. Leon, 468 U.S. 897, 918, 926 (1984) and finds that: "Leon contains not the slightest suggestion, however, that the same deference ought apply when magistrate judges determine their own jurisdiction. Indeed, the Supreme Court's conclusion presupposes that the issuing magistrate judge was authorized to issue the challenged warrant." *Levin* at slip op. p. 25.

2. Relief Under Rule 41

Under Rule 41 suppression is only an available remedy if the violation is considered to be substantive and not merely procedural. The lack of authority by the issuing magistrate cannot be considered procedural or ministerial. The search is the equivalent of a search without a warrant.

This point is reiterated a number of times in this article and in both *Levin* and *Croghan.* Counsel should never acquiesce to terminology that diminishes this fact.

3. Even if the Issuance of the NIT Warrant Was a Ministerial Error There Was Prejudice to the Defendant and the Evidence Must Be Suppressed

Even if the Rule 41(b) violation was ministerial, suppression would still be appropriate, if the defendant demonstrates that he suffered prejudice. The fact that in the absence of the NIT Warrant no search would have occurred is proof in and of itself of prejudice to the defendant. See Levin at slip op. p. 22-23. In the words of Judge Pratt:

> It is clear in this case that neither the search pursuant to the NIT Warrant nor the searches pursuant to the Iowa Warrants would have occurred without the violation of Rule 41(b). Had Rule 41 been complied with, law enforcement would not have obtained Defendants' IP addresses, would not have been able to link those IP addresses to Defendants through subsequent investigation and [*26] the use of administrative subpoenas, and would not have had sufficient probable cause to obtain the Iowa Warrants. Thus, Defendants have satisfied their burden to prove that they were prejudiced by the Rule 41(b) violation. Suppression is an appropriate means to deter law enforcement from seeking warrants from judges lacking jurisdiction to issue them, and this deterrence function outweighs the societal costs associated with suppression.

Croghan slip op. at p. 10. Technology is changing the manner in which the police investigate crimes. While technology has made it easier for some people to hide misdeeds it has also become ubiquitous. We store our lives on our computers. Incursions by the government into those computers should be supported by a warrant issued by a judicial officer who is recognized to have the sufficient office and authority to make such important decisions.

III. More than One Way to Skin the Cat – *United States v. Michaud* and the Exclusion of Evidence through Discovery Litigation

In *United States v. Michaud,* No 15-cr-05351-RJB, the defendant's motion to suppress the Playpen NIT warrant was denied in the Western District of Washington. Undeterred, the defendant managed to get the results of the NIT search and seizure excluded through a successful course of discovery litigation.

In *Michaud,* the defense filed a motion to compel discovery of the programming code that powered the NIT in the Playpen cases. *See United States v. Michaud*, No. 15-cr-5351-RJB, Doc. 54 (W.D. Wash. Nov. 20, 2015.) The motion was preceded by a series of discovery letters to the Government with a comprehensive list of required discovery. *See Michaud,* Doc. 54-1. In the motion to compel Michaud set forth the following reasons to compel the discovery:

1. The forensic information and programming code are relevant to the motion to suppress and the ability of the defendant to require a *Franks* hearing.

2. The forensic information and programming code is necessary so that the defendant's computer forensics expert can independently determine the full extent of the information the Government seized from Mr. Michaud's computer when it deployed the NIT; whether the NIT interfered with or compromised any data or computer functions; and whether the Government's representations about how the NIT works in its warrant applications were complete and accurate.

3. Citing a case involving a prior NIT warrant, *United States v. Cottom*, 99 Fed, R. Evid. Serv. 256 D. Neb., 2015), the Government had previously made copies of a NIT programming code available for inspection and forensic analysis.

4. The forensic information and programming code are relevant to the Defendant's motion to dismiss based on the outrageous governmental conduct of operating a child pornography website and purveying child pornography to the public.

5. The forensic information and programming code are relevant to the Government's claims that agents acted in good faith reliance on the NIT warrant.

See Michaud, Doc. 54. The Government responded to the motion asserting that the discovery sought was not material to the preparation of a defense and stating that the material sought would net be material under F.R.Cr.P. 16 (a)(1)(E). The Government also argued that the release of the NIT code in the Cottom case involved an earlier case and different NIT than the one used to prosecute Michaud. The Government's final claim was that a qualified law enforcement privilege attached to the NIT because its disclosure "would be harmful to the public interest" because disclosure would diminish its effectiveness in future investigations, In its opposition to the motion to compel the government likened the law enforcement privilege to the informer's privilege which stems from *United States v. Roviaro*, 353 U.S. 53, 59 (1957). *See generally Michaud*, Doc. 74 (W.D. Wash. Dec. 4, 2015.)

During the course of the discovery litigation the Government agreed to provide the NIT programming code and the Court, for the most part granted the motion to compel disclosure of the balance of the information sought. However, the Government had second thoughts about the disclosure of the NIT programming code and refused to provide it triggering a third round of discovery motions. After oral argument the trial court granted the motion and ordered the Government to produce the NIT programming code and additional information. *See Michaud*, Doc. 161. On the record the court stated:

> THE COURT: Well, first I am satisfied that the defense has shown materiality here to preparing the defense. I don't need to discuss that in depth, in my view. I think the papers speak for themselves. And it may be a blind alley, but we won't know until the defense can look at the details of what was done.
>
> ….
>
> It is my opinion that the protective order in place is sufficient to protect this information, and it is my judgment that the motion should be granted
>
> …
>
> Now, you know, behind that ruling is this: The government hacked into a whole lot of computers on the strength of a very questionable search warrant. I ruled on the admissibility of that in what I considered to be a very narrow ruling.

> 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. And the government should respond under seal and under the protective order, but the government should respond and say here’s how we did it.
>
> So, you know, I guess what I am saying is that this whole thing didn’t seem that
>
> complex to me . . . .

Michaud, Doc. 162 at p.17-19. Further litigation stemmed from Government motions for reconsideration which resulted in further hearings. The court eventually reviewed the information in camera an d determined that the law enforcement privilege applied to the NIT programming code. Nevertheless the Court maintained that the information was material to the preparation of the defense:

> Well, this question of relevance or materiality or what should be turned over to the defense under the rules is what we are talking about here. I have not changed my opinion on that based on what has been presented here on this motion to reconsider.
>
> I was earlier, and still am, impressed by the material from Mr. [Tsyrklevich]. It seems to me, as I said before, that the defense has the right to know what tools you used to hack into his computer.
>
> I am impressed -- I don't think anything that the government has said has overcome that showing. The response to that is substantially that the defense hasn't proved what they don't know -- they haven't proved what they don't know, but what they want to know is what they don't know so they can determine what defenses are appropriate, or, I might say, under the Ninth Circuit cases, in particular the *Hernandez-Meza* case, which is 720 F.3d 760, they have a right to consider this information partly to determine whether it should lead to a plea, whether there are any defenses. And I think they have a right to that information.

Michaud, Doc. 204 at 33. In one of its many orders the court stated:

> 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 justifiable right not to turn the information over to the defense?

Michaud, Doc. 205 p. 5. Subsequent hearings were held in May of 2016. The defense maintained with dogged determination that dismissal was the appropriate remedy. The record in the docket contains several sealed pleadings which is understandable considering that the court found the law enforcement privilege applied to the NIT. Ultimately the court denied the motion to dismiss but ordered that "evidence of the N.I.T., the search warrant issued based on the N.I.T., and the fruits of that warrant should be excluded and should not be offered in evidence at trial." *Michaud*, Doc. 212.

Sheer perseverance appears to be the winning attribute displayed by the defense team in Michaud. However, their success can also be attributed to a number of wise choices that were made during the course of the litigation. **First it is imperative that a qualified and persuasive computer forensics expert be hired at the outset of these cases.** The defense expert testimony was impressive to the trial court and clearly contributed to the court's concern about materiality. The defense expert exposed the *ipse dixit* nature of the government responses to the discovery requests and provided a measure of assurance for the court that the information sought was material. **Second, never accept the Government's traditional response that it will comply with its Rule 16 and Brady obligations.** "The defendant is not required to accept the government's assurances that reviewing the N.I.T. code will yield no helpful information. The government asserts that the N.I.T. code will not be helpful to the defense, but that information may well, in the hands of a defense lawyer with a fertile mind, be a treasure trove of exculpatory evidence." *Michaud*, Doc. 205, p. 4. **Third, make your discovery requests specific, make them early and make them often.** The Michaud defense wrote three extensive letters to the prosecution team seeking specific information. The repetition of your request may result in concessions from the prosecutor and may underscore the importance of the discovery for your trial judge. **Fourth, don't give up when the Government claims a privilege.** Michaud demonstrates that it is possible for information to be both privileged and material to the defense. Demand a remedy when the government claims privilege. You may not get the dismissal you seek but you may still be surprised at your success. **Fifth, request a hearing at every opportunity.** Give the court the opportunity to hear from you and your expert. Give the court the opportunity to talk through the facts and the opportunity to understand how the issues are relevant and material to your case. But also let the court know when the Government's conduct is outrageous. **Finally, never quit.**

IV. Suppressing Digital Evidence Reviewed by the National Center for Exploited and Missing Children (NCMEC)

The National Center for Exploited and Missing Children (NCMEC) has assisted law enforcement for many years in the investigation of child pornography offenses. Starting at least after the Supreme Court decision in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) NCMEC has maintained a database of child pornography images in which the children are identified. The database is used to counter defense claims that the images may not be of real children.   As computer technology has advanced so too has the ability of NCMEC to identify child pornography images transmitted through the internet. 18 USC § 2258A (a) (1) requires electronic communication service providers to report all electronic communications that appear to contain child pornography directly to NCMEC.

Electronic communications containing child pornography are usually identified by a hash value that is assigned to each attachment to an electronic communication. The hash value is compared to hash values for known child pornography. If a hash value matches, the ISP is required to make an immediate report to NCMEC.

So what exactly is NCMEC? In a recent case the Tenth Circuit that question has been answered. Although ostensibly a private corporation, NCMEC is both a governmental entity and a government agent. *See United States v. Ackerman*, ____F.3d ____ (10th Cir., August 5, 2016.) In *Ackerman* the ISP known as AOL identified an electronic communication containing four attachments. AOL reviewed and compared the hash value of one of the attachments, determined that there was apparent child pornography and forwarded the email and attachments to NCMEC through the CyberTipline. NCMEC employees then opened the email and viewed each of the attachments and determined that each contained child pornography. NCMEC then notified local law enforcement officials who obtained a search warrant based on the NCMEC report, searched Mr. Ackerman's computer and arrested him. He was charged with possession and distribution of child pornography and entered a conditional guilty plea after his motion to suppress was denied based on the trial court's ruling that NCMEC was not a government agent.

The Tenth Circuit defined the issue as follows:

> But the Fourth Amendment only protects against unreasonable searches undertaken by the government or its agents — not private parties. So Mr. Ackerman's motion raises the question: does NCMEC qualify as a governmental entity or agent? Even if it does, a second hard question remains. The Supreme Court's "private search" doctrine suggests the government doesn't conduct a Fourth Amendment "search" when it merely repeats an investigation already conducted by a private party like AOL. Which raises this question: did NCMEC simply repeat or did it exceed the scope of AOL's investigation?

*Ackerman***,** slip op. p. 4. In determining the question the Tenth Circuit undertook a wide ranging review of the history of corporate law as it relates to governmental entities. Starting with *Trustees of Dartmouth College v. Woodward*, 17 U.S. (4 Wheat.) 518, 668-69 (1819) circling back to ancient English law, including Blackstone's Commentaries the court came to the modern day conclusion that NCMEC is indeed a governmental entity. More importantly the Court recognized that NCMEC is a governmental *law enforcement* agency. “NCMEC’s two primary authorizing statutes — 18 U.S.C. § 2258A and 42 U.S.C. § 5773(b) — mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person.” *Ackerman* slip op. p. 6. The Ackerman Court likened NCMEC to Amtrak. In *Lebron v. Nat’l R.R. Passenger Corp*., 513 U.S. 374, 399 (1995); *Dep’t of Transp. v. Ass’n of Am. R.Rs. (DOT),* 135 S. Ct. 1225, 1233 (2015) the Supreme Court held that Amtrak, a publicly owned company is, in fact, a governmental entity.

The *Ackerman* court also determined that NCMEC is a government agent. Under either of the two prevalent tests of whether a person is a government agent for Fourth Amendment purposes, NCMEC fits the bill. *See Ackerman,* slip op. p. 19 – 21.

After determining that NCMEC is both a government entity and a government agent the *Ackerman* Court determined that the opening of the email was, in fact, a search. “The undisputed facts show, too, that NCMEC opened Mr. Ackerman’s email, found four attachments, and proceeded to view each of them. And that sort of rummaging through private papers or effects would seem pretty obviously a “search.” After all, if opening and reviewing “physical” mail is generally a “search” — and it is, *Ex Parte Jackson*, 96 U.S. 727, 733 (1877); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) — why not “virtual” mail too?” *Ackerman*, slip op. p. 25-26. Noting that the district court (and apparently the Government) agreed that Ackerman had a reasonable expectation of privacy in his e-mail the Tenth Circuit did not attempt to plumb the depth of the “third party doctrine” and its potential application to e-mail. However the Court did address the “private search doctrine” which blesses searches by government agents that repeat the search conducted by a private party. In this case the Government argued that NCMEC did nothing more that AOL had previously done. The Court disagreed finding that NCMEC actually opened the e-mail and viewed not just one, but four, attachments for child pornography. According to the Court "as far as anyone knew" the e-mail and the attachments could have contained any kind of non-contraband material.

The *Ackerman* Court also noted that the "reasonable expectation of privacy test" from *Katz v. United States,* 389 U.S. 347 (1967) is no longer the sole determinant of the reasonableness of a search. The Court cited *United States v. Jones,* 132 S. Ct. 945 (2012), for the proposition that the reasonableness of a search can be based "on a reasonable expectation of privacy or when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects") for the purpose of obtaining information." *Ackerman,* slip op. p. 25-26. In short the Court found that NCMEC is the government and that NCMEC conducted a search. Because the Government did not posit the arguments the *Ackerman* Court did not consider whether the NCMEC search was justifiable as reasonable and under the special needs doctrine or whether the good faith exception should apply to the search. The district courts order was reversed and the matter was remanded to the district court. It is likely that the Government will take the Court's advice and attempt to rely on a better theory to pursue admissibility of the *Ackerman* email and attachments.

The *Ackerman* Court leaves the reader with the following:

> So with that, our encounter with this case comes to an end — at least for now. Surely hard questions remain to be resolved on remand, not least the question whether the third-party doctrine might preclude Mr. Ackerman's claim to the Fourth Amendment's application, a question the government has preserved and the district court and we have reserved. But about one thing we can be very certain. There can be no doubt that NCMEC does important work and that its work can continue without interruption. After all, it could be that the third-party doctrine will preclude motions to suppress like Mr. Ackerman's. Or that

> changes in how reports are submitted or reviewed might allow NCMEC to access attachments with matching hash values directly, without reviewing email correspondence or other attachments with possibly private, noncontraband content — and in this way perhaps bring the government closer to a successful invocation of the private search doctrine. Or it may be possible that the government could cite exigent circumstances or attenuation doctrine or special needs doctrine or the good faith exception to excuse warrantless searches or avoid suppression in at least some cases. But even if not a single one of these potential scenarios plays out — and we do not mean to prejudge any of them — we are confident that NCMEC's law enforcement partners will struggle not at all to obtain warrants to open emails when the facts in hand suggest, as they surely did here, that a crime against a child has taken place.

Ackerman slip op. at p. 35-36. The confidence of the Tenth Circuit notwithstanding criminal defense lawyers should be able to use *Ackerman* as a comprehensive and credible response to claims that NCMEC is not a government agent or entity – the first step in seeking suppression.

I'll be there on time and I'll pay the cost,
For wanting things that can only be found
In the darkness on the edge of town.