A HOOVER INSTITUTION ESSAY

The Elephant in the Room: Addressing Child Exploitation and Going Dark

SUSAN HENNESSEY

Aegis Paper Series No. 1701

There is an unacknowledged Venn diagram at the heart of the Going Dark[1] debate. Circle A represents crimes for which various manifestations of technology pose extreme challenges to law enforcement investigations: for example, computer offenses that take place exclusively online or technology-based narcotics trafficking and money laundering. Circle B represents crimes for which society demands an exceptionally high level of effective prevention, investigation, and prosecution: violent offenses with identifiable victims like murder or rape. This is not to say Circle A crimes are unimportant—only that, taken alone, society is more inclined to view the security benefits of robust encryption as outweighing the net harms. Likewise, it is certainly true that investigation of Circle B crimes can be impeded by encryption and other technology. But more often than not, law enforcement has at least some other avenues of obtaining evidence, such as from a crime scene or from witnesses.

At the intersection of the Venn diagram are two sets of crimes where encryption technology poses serious law enforcement problems *and* for which society expresses an especially low tolerance: terrorism and child sexual exploitation.[2] Our public dialogue focuses relentlessly on one of these sets of crime, and it largely ignores the other.

Indeed, while the problem of encryption and terrorism investigations gets plenty of play in the public debate, the specific problems of child sexual exploitation receive relatively little attention beyond oblique references. This is perverse. The latter is a problem of immense global scope; it is deeply entangled with technology; and it animates law enforcement's strongest interests in solving the Going Dark problem. There are many more child exploitation cases than there are major terrorism investigations, and they are much more likely to involve technologies of encryption pervasively.

Susan Hennessey is a fellow in National Security Law in Governance Studies at the Brookings Institution and managing editor of *Lawfare.* Special thanks to Benjamin Wittes, Jack Goldsmith, Helen Klein Murillo, and the Hoover Working Group on National Security, Technology, and Law for their support and input and to representatives from the Department of Justice and Federal Bureau of Investigation for their invaluable insights and assistance.

There are a number of additional reasons to focus more of the Going Dark conversation on child sexual abuse than we currently do. Because child sexual exploitation is relatively common, while terrorism is relatively uncommon, the majority of relevant case law is likely to be created in the context of child exploitation. Second, because child predators have historically been at the cutting edge of using technology to thwart law enforcement, the challenges and solutions that arise in this context may serve as a preview for those that will later appear in relation to terrorism and other serious crimes.

The problems of child sexual exploitation are immediate and real. Whereas with respect to terrorism cases we often end up hypothesizing how law enforcement and policy makers will respond to "the next big attack," in the child exploitation context the next attack is happening literally every day. Technology has facilitated a dramatic increase in the trafficking of child sexual abuse images and a concomitant increase in the severity of depicted abuse. Children as young as infants and toddlers are raped or otherwise abused on camera; those images are routinely shared among a community of offenders; and those offenders deploy technologies that make it difficult or impossible to discover the perpetrators, prosecute their crimes, or identify and rescue victims.

Faced with this reality, civil libertarians and privacy advocates have been loath to allow for any latitude, either in regulating encryption or in facilitating work-arounds like lawful hacking. This absolutist strategy is, I shall argue here, untenable over the long term. The simple reality is that if we are not going to regulate encryption, then we are going to have to do something else to address these issues.

In this paper, I describe the particular impacts of Going Dark on the prevention, investigation, and prosecution of child sexual abuse crimes; and I make the case for lawful hacking as a promising solution, identifying the legal questions that must be addressed for hacking to be a practical and realistic response. I start by reviewing the available statistics related to quantifying the scope of child sexual abuse and related materials. The numbers paint an undeniably alarming portrait of their scope and severity. I then address the specific features of Going Dark, both technical and otherwise, in the context of investigating child exploitation crimes. Taken together, these features make child sexual exploitation crimes easier to commit and more difficult to detect.

I argue that lawful hacking, wherein the government exploits existing software vulnerabilities to circumvent security, is a necessary element of a Going Dark solution. I then examine the various legal controversies that must ultimately be resolved for lawful hacking to be a solution in practical terms. First, I argue that the recently resolved controversy over Rule 41 of the Federal Rules of Criminal Procedure

encourages the use of warrants and that warrants for large-scale hacking operations can satisfy all constitutional requirements, including particularity and probable cause.

I then examine the issue of vulnerability disclosure, both at a policy level and as a matter of constitutional and procedural right in criminal trials. I recommend mechanisms to ensure that disclosure requirements do not undermine the efficacy of lawful hacking. Finally, I address the complex international features of Going Dark and child sexual exploitation investigations and suggest those challenges could be best addressed through a pragmatic framework rooted in commonly understood offenses.

The Scope of Child Sexual Abuse and Child Sexual Abuse Materials

It is difficult to precisely quantify the scale of the problem of child sexual abuse and abuse images. But the estimated rates of hands-on sexual abuse of children are staggering. Approximately one in ten children—one in seven girls and one in twenty-five boys—will be subject to a contact sexual offense before reaching the age of eighteen.[3] Although many people perceive adult sexual assault as a more common offense, nearly 70 percent of all reported sexual assaults involve a victim under the age of eighteen. In crimes of rape involving penetration, 29 percent of rape victims are between twelve and seventeen years old, and 15 percent of victims are younger than twelve.[4] Because only around 38 percent of child victims disclose the fact that they have been sexually assaulted, these numbers almost certainly dramatically understate the problem.[5]

Only some instances of child sexual abuse are memorialized in images; therefore, the numbers related to abuse images represent only a fraction of child victims. But even within this subset, immense numbers of both victims and offenders are represented. A review of available metrics, both general and related to specific operations, reveals that the problem is very serious and rapidly getting worse. Consider the following:

- The National Center for Missing and Exploited Children (NCMEC) CyberTipline has received 8.4 million reports since 1998—nearly half of those in 2015 alone, the most recent year with available metrics.[6] Since 2002, NCMEC has reviewed more than 160 million images and videos of suspected child abuse.[7] Between 2005 and 2009, the Victim Identification Program saw a 432 percent increase in the number of files submitted.[8] In 2013, it reviewed twenty-two million images and videos—a 5,000 percent increase from 2007.[9] In 2015, the number of images and videos reviewed grew to twenty-six million.[10]

- NCMEC estimates that, since 2002, more than 10,500 minor victims depicted in child sexual abuse images have been identified and located by law enforcement.[11]

- Operation Predator, run by the Department of Homeland Security, focuses on disrupting and dismantling the production and distribution of child sexual abuse materials and countering child sex tourism.[12] Since 2003, Operation Predator has led to 35,000 investigations and the arrests of more than 13,000 child predators.[13] Between 2012 and 2015 alone, the group arrested more than 8,500 suspected child predators and identified 3,259 child victims.[14]

- Between 2010 and 2015, the US Marshals Service received approximately 10,000 requests from law enforcement for assistance in fugitive cases involving the sexual exploitation of a child.[15] Working with NCMEC in the same period, the Marshals Service recovered 427 children.[16]

- Between 2010 and 2015, the US Postal Inspection Service arrested more than five hundred offenders who used the US mail to facilitate or exchange materials related to the sexual exploitation of a child.[17]

- The Department of Justice Child Exploitation and Obscenity Section (CEOS) led fourteen national and international operations between 2013 and 2015, resulting in the investigation of 2,600 individuals in the United States and more than 8,000 individuals abroad.[18]

- In 2014, the US Attorneys' offices filed 3,248 indictments for child sexual exploitation against 3,422 defendants, representing a 31 percent increase over 2010.[19] In the period between 1994 and 2006, the US Attorneys' offices had already seen an 82.8 percent increase in such cases.[20]

- International studies mirror US estimates demonstrating the proliferating global threat. A 2010 UNICEF report estimated that more than four million websites feature sexually exploited minors. Over time, the number of child sexual abuse material websites has been growing.[21] By conservative estimates, more than two hundred new images of sexually exploited minors are circulated daily. UNICEF estimates that between three billion and twenty billion dollars per year are generated from the production and distribution of child sexual abuse images.[22] A United Nations report from July 2009 offered an estimate that, at the time, approximately 750,000 sexual predators used "the Internet to try to make contact with children for the purpose of sexually exploiting them."[23] Today, the number is not considered measurable.

Beyond the growing numbers of images, victims, and offenders, law enforcement officers around the world report that child sexual abuse images are increasing in severity—depicting more violence and younger victims.

Although it is difficult to differentiate among "the worst of the worst," the age of the victim is one common marker in measuring severity. According to the US Department of Justice, "Child advocate personnel across the United States report that the ages of victims depicted in child pornography have significantly decreased in the past few years."[24] In a 2010 National Drug Intelligence Center (NDIC) survey of law enforcement personnel, "82 percent of respondents reported [minor victims] in all age brackets, 51 percent reported that most investigations involved prepubescent children, and 67 percent reported that victims [were] getting younger."[25] When the same survey was administered in 2015, respondents reported that the "average age of child victims depicted in child pornography" had continued to decrease over the preceding five years.[26] The trends are "supported with significant feedback detailing that it is now routine for child pornography investigations to include files depicting the sexual exploitation of infants and toddlers."[27] Disturbingly, law enforcement expects the trend toward younger victims to stabilize because victims simply cannot get any younger; reported images now extend to "children as young as days old."[28]

In addition to younger victims, the "2016 National Strategy survey shows that offenders also have increased their demand for more depraved and egregious content."[29] According to the Justice Department, the greater availability of child sexual exploitation materials has stimulated the demand and production of even more extreme, sadistic, and violent images of children and infants.[30] This content appears "most voluminously" on Tor.[31] Thirty percent of 2016 *National Strategy* survey respondents indicated an increase in the level of violence depicted within sexual abuse images.[32]

Indicators of the trend toward increasing violence date back to the early 2000s. According to the 2010 *National Strategy,* "U.S. Sentencing Commission data between 2002 and 2008 shows a 65 percent increase during that period regarding enhancements for sadistic, masochistic, or violent images."[33] And trends toward increasing depravity and violence also appear in the 2010 survey results.[34] Although some respondents reported there was no change in violence, no respondents reported decreased violence.[35]

Unsurprisingly, law enforcement officers outside the United States also report facing significant obstacles in investigating and prosecuting these crimes. Canadian officials, for example, recently warned that online child sexual exploitation had reached "a level of epidemic proportions" and that a national tip line for reporting suspected abuse had experienced an increase in reporting not only in the number of incidents but also "increases with respect to the severity of the acts and images of very young children."[36]

The bottom line here is that the problem exists, it is of an immense scale, and by most indicators it is getting worse. Then attorney general Eric Holder summarized the issue at a

2011 conference on combating child exploitation: "We've . . . seen a historic rise in the distribution of child pornography, in the number of images being shared online, and in the level of violence associated with child exploitation and sexual abuse crimes. Tragically, the only place we've seen a decrease is in the age of victims. This is—quite simply—unacceptable."[37]

Holder referenced a value that is nearly universally shared: we cannot and will not, as a society, passively tolerate these kinds of crimes against children. Holder went on to say, "But, together, we are fighting back." That fight—against both people who hurt children and the use of technologies to facilitate and conceal those crimes—is the front line of Going Dark. And that fight, which Holder called "our nation's most sacred pledge," is one the government isn't walking away from.

The Features of Going Dark in the Context of Child Sexual Exploitation

Although law enforcement faces numerous challenges in countering child sexual exploitation, rapidly advancing technologies pose the most urgent concerns. According to the Department of Justice, "for every innocuous need technology fills for law-abiding citizens, online sex offenders will find a malicious use."[38] Technological advancements pose two related but distinct problem types. First, offenders use readily accessible and increasingly sophisticated technology to more easily produce, access, store, and transmit sexual abuse images. Law enforcement officials report a significant increase in the use of known distribution platforms, including "instant messaging services, peer-to-peer networks, online file-storage services (cloud), anonymous networks, photo-sharing apps, and mobile-only apps" as well as an increase in the use of "e-mail and photo-sharing websites to distribute child pornography."[39] The only distribution platform where there has been an observed decrease in use is traditional mail and postal services.[40]

Second, offenders use increasingly sophisticated tools and techniques to evade detection. The 2016 DOJ National Survey found that "more than 38% of survey respondents reported a significant increase in the technical sophistication and expertise of child pornography offenders," with similar numbers reporting increases in the use of anonymization tools and encryption.[41]

Although the features of Going Dark regarding child sexual exploitation are varied, the most significant technological issues arise in the context of device encryption, anonymization, and hidden services.

Device Encryption

Even when probable offenders are identified, investigators are often unable to access content where contraband materials are stored on encrypted devices such as laptops, smartphones, and external hard drives. Strong encryption makes accessing these devices without knowing the key exceedingly difficult and often impossible. When the suspect refuses to disclose the key or claims to have forgotten it,[42] several problems result. First, obtaining a conviction for possession of contraband child pornography is, in some cases, impossible without being able to access the images in question. Second, even where there is available evidence sufficient to support a conviction, being unable to gain access to all contraband images in the defendant's possession prevents the government from establishing whether the individual is a repeat offender or is subject to higher mandatory minimum sentences for aggravating factors. More important, encryption can thwart the identification of "hands-on" offenses, denying unidentified victims justice and desperately needed recovery support.

Finally, device encryption hinders the enormous amount of productive international cooperation that depends on sharing images. Large databases house hundreds of thousands of pictures and videos; investigators worldwide can access these systems to cross-check for victim identification or evidence of connections between perpetrators. Often, single individuals will possess only a few of the multiple images or materials created during a production offense. Taken on their own, the pictures might not present sufficient information to provide an identification. But when the series is aggregated, clues can be pieced together. Some of the most important methods of victim identification are low-tech and depend on individual investigators examining images for clues as to probable jurisdiction.

Increasingly sophisticated device encryption is widely available and is often enabled by default. This lowers the threshold of skills required to participate in the production, consumption, and exchange of child sexual abuse materials undetected, allowing a broader group of offenders to freely operate. In the recent past, technology companies retained the capacity to access data encrypted on devices and would do so when presented with both the device and a court order for the contents. Companies, however, are increasingly offering forms of encryption that put data beyond their own reach, even when served with lawful process. This prevents law enforcement from accessing the contents for the purposes of investigation, prosecution, sentencing enhancement, and victim identification. Furthermore, the knowledge of this heightened security emboldens offenders. Both research and law enforcement observations suggest that this sense of offender security, afforded by encryption and other forms of anonymity, contributes to trends toward more depraved and violent

offenses and increasingly younger victims by eliminating the inhibiting fear of being caught.[43]

Anonymization

Another significant Going Dark impact arises from the use of anonymization networks that thwart investigative techniques aimed at locating offenders. Tor is one commonly utilized network for child exploitation offenders. Tor, in effect, conceals the genuine Internet protocol (IP) address of the computer visiting a website.[44] An IP address identifies a device communicating with a network, somewhat similar to a phone number or street address. When an IP is identified, law enforcement can discover the physical location of a computer accessing a particular website at a particular time. Unlike ordinary browsers, Tor relays traffic from a device through a series of intermediary nodes.[45] A device's genuine IP address is revealed to the original node, but by the time the traffic reaches the intended destination, it is not possible to trace the source back to the original user. Although Tor is used as a censorship circumvention tool and affords privacy protections to individuals engaged in sensitive communications online, it is also commonly used by child sexual predators to evade detection.

Accessing child pornography with the intent to view it is a felony.[46] However, even when law enforcement agents identify websites hosting child sexual abuse images—and are able to observe offenders' accessing or uploading contraband images in violation of federal law—they are unable to identify the physical locations of the perpetrators' computers, and thus cannot execute warrants to obtain evidence, identify victims, and arrest and prosecute dangerous criminals.

As with device encryption, anonymity appears to embolden offenders to commit more egregious offenses and to share massive quantities of child sexual abuse images. Law enforcement agencies report that depictions of the most violent and sadistic acts perpetrated against the youngest victims appear "most voluminously on the Tor anonymous network."[47]

Hidden Services and Offender Communities

A distinct element of Tor, known as "hidden services," features prominently in child sexual abuse offenders' ability to evade justice.[48] Tor hidden services allow users to offer services and host websites while hiding their locations. Hidden services are not visible to traditional search engines; an individual must know the secret "onion address" to access the hidden site using the Tor browser.[49] This has led to the proliferation of community websites dedicated to the sharing of child sexual abuse materials as well as

to the discussion, normalization, and exchange of advice about hands-on abuse of children. Federal law enforcement reports a "mass migration of child pornography offenders" to such sites.[50]

These offender communities are deeply problematic to law enforcement for a number of reasons. The groups exchange massive volumes of child sexual abuse materials and have hundreds of thousands of users. An FBI investigation into a single website hosted on Tor revealed that there were approximately two hundred thousand registered users; one hundred thousand individuals accessed the site during a twelve-day period.[51]

These hidden service sites allow for closed and protected online spaces, which are difficult to locate and identify. Within these communities, members are carefully vetted to guard against law enforcement undercover infiltration. Offenders meet "like-minded people across the globe" to exchange child sexual abuse images, to discuss best practices for grooming, recruiting, and exploiting victims, and to trade operational security tips and technological methods to evade detection.[52]

Through these forums members normalize and collectively reinforce one another's sexual interest in children, encourage others to act on deviant sexual interests, and assist in targeting victims. The forums facilitate the live-streaming of abuse as well as "made-to-trade" materials, wherein offenders document particular abuse tailored to the interests of other community members.

Additional Going Dark Factors

Although the analysis and recommendations in this paper focus on those elements that can be mitigated at the technical level, it is important to recognize the wide spectrum of challenges facing those who investigate and prosecute these crimes and work to identify and rescue victims. The various pressures on child sexual exploitation include many forms of technology, as well as corporate policies and legal precedent. Below is a non-exhaustive list of factors.

- **Live-Streaming of Abuse, Sextortion, and Webcams:** There is an increased trend toward live-streaming where individuals pay to watch the live abuse of a child via a video streaming service. This is an especially pernicious problem because the real-time nature makes detecting such abuse incredibly difficult and digital evidence is not left behind after the fact. Beyond the commercial market for abuse materials, offenders also increasingly use webcam video to view victims in real time to avoid producing or storing images or videos that could later be discovered by law enforcement.[53] Similarly pernicious is the phenomenon

of "sextortion," by which perpetrators threaten to make public stolen or directly obtained illicit images to extort the victim into producing additional images.[54]

- **Countersurveillance methods:** Thanks in part to offender community education, offenders are increasingly using "throw-away" free e-mail accounts and secure e-mail accounts to facilitate exchange of and access to materials. Predators are known to develop operational security methods by tracking cases in the news and researching topics presented at law enforcement conferences. Once an effective method is developed it is widely shared among offenders.[55] Child pornography producers are also taking new efforts to obscure the faces of offenders and victims, to remove any items that might offer clues on location, and to otherwise "scrub" or edit abuse materials for the purpose of hindering law enforcement investigations.

- **Internet Service Provider (ISP) Policies on Data Retention:** Even where IP addresses can be determined, when ISPs do not retain identifying information, the offenders have the benefit of unintentional anonymization.[56] In the United States, some providers retain the relevant information for as little as a few days, which often hinders investigations.[57] No federal laws require providers to store identifying IP information for any period of time.[58]

- **Mobile Devices and Applications:** Mobile devices can be used to photograph or film a child being sexually abused, access child sexual abuse material stored in remote locations, and stream video of child sexual abuse. Offenders have also rushed to capitalize on mobile technologies that allow anonymous production and sharing of videos to entice naïve minors to produce and share explicit images of themselves.[59]

- **Evidence Located in Multiple Jurisdictions:** Increasingly, both individuals and evidence related to child sexual exploitation offenses are located in multiple countries. Coordinating international investigations and obtaining evidence for other sovereigns is complex and time-consuming. And the number of countries where offenders, victims, and evidence might be located increases as Internet and mobile technologies connect more people in the developing world.[60]

- **Remote Cloud Storage:** Remote cloud storage makes it possible for individuals to consume child sexual abuse materials without needing to possess contraband in their homes or offices where it might be discovered or seized by law enforcement.[61]

Cloud storage allows for the inexpensive storage of thousands of images, which can be accessed from anywhere, while strong encryption prevents law enforcement access.

- **Free or Unsecured Wi-Fi and Public Access Points:** Open and unsecured Internet access points can make it difficult to match individual users to the networks they use to access contraband.

- **Peer-to-peer (P2P) Networks:** Peer-to-peer networks are increasingly used as child sexual abuse material distribution platforms. It is impossible to definitively quantify the number of computers or users sharing child exploitation material via P2P. One study, however, estimated that 3 in 10,000 users on the five most common networks were sharing child pornography images each month.[62] A different study of a popular P2P network found more than 30 percent of searches were related to child sexual abuse materials.[63]

- **Evidence-eliminating Software:** Sophisticated software is now available to eliminate images and other evidence from computers and hard drives, impeding later forensic analysis.

- **Corporate Policies on Data Sharing and Legal Process Notification:** Changes in corporate policies regarding information-sharing with law enforcement and the timing of decisions on when to notify customers about the receipt of legal process have also generally increased the difficulty of child sexual exploitation investigations.[64]

- **Stronger Security Defaults:** The technical challenges posed by encryption have increased exponentially with the proliferation of encryption and strong security settings enabled by default. Although these changes extend meaningful security benefits to ordinary users, they also reduce the number of instances in which offenders make mistakes. Importantly, these defaults extend sophisticated security not only to the offenders themselves—who might otherwise avail themselves of technological protections—but also to the universe of individuals connected to them who might have information relevant to an ongoing investigation.

- **Digital Currencies:** The spread of digital currencies provides offenders with additional layers of identity protection by avoiding the need to rely on traditional credit cards or other methods of payment tied to true identities.[65]

The Case for Lawful Hacking to Combat Child Sexual Abuse

Thus far, the Going Dark debate has focused largely on the merits of decryption mandates or "backdoor" access for law enforcement. But within those discussions, lawful hacking has emerged as one potential alternative solution.[66] Instead of creating additional vulnerabilities to an already fragile security ecosystem in the form of exceptional access, commentators have argued that law enforcement should exploit existing vulnerabilities in software and hardware.[67]

Child sexual predators are technologically sophisticated and security-focused, which means they are likely impervious to legislative efforts to establish exceptional access or standards for defaults. Consequently, child sexual abuse investigation is an area where government hacking is urgently needed. It is also a useful testing ground for the feasibility of this solution to Going Dark in broader contexts. Although lawful hacking cannot hope to resolve all of the issues surrounding technology and child exploitation investigations, it should be viewed as a necessary element of a comprehensive response. First, successful lawful hacking can lead to the identification of offenders and the rescue of child victims. Second, developing lawful hacking techniques will reduce the sense of security and comfort offenders feel in accessing and distributing child sexual abuse materials, which could help stem the trend toward more severe and egregious content. Third, lawful hacking can and should be targeted at dismantling offender communities that proliferate on hidden services and other platforms. Experts believe these communities are responsible for the observed increase in the severity of depicted abuse and for disseminating effective countermeasures to avoid detection.[68]

If lawful hacking is going to offer a meaningful method to respond to these crimes—as opposed to being a diversionary tactic intended to delay government action on other fronts—then a number of legal, operational, and policy questions must be addressed.

The Playpen NIT as a Legal Roadmap for Lawful Hacking

The ultimate utility of lawful hacking will depend as much on legal developments as on technological ones. Many of the relevant questions are currently before multiple federal courts in a series of prosecutions stemming from an FBI child exploitation investigation. It is not coincidental that courts are confronting novel legal questions of government hacking in the context of child sexual exploitation cases. These cases offer further evidence that child exploitation crimes are an urgent and growing concern for law enforcement and are an area where traditional investigative techniques are easily circumvented.

A 2015 FBI operation against the child pornography website Playpen has led to at least two hundred criminal prosecutions in dozens of federal districts across the United States.[69] Those cases provide a useful road map to understanding the fundamental legal issues underlying lawful hacking.

In August 2014, a foreign law enforcement agency alerted the FBI to a website dedicated to the distribution of child sexual abuse materials believed to be based in the United States. The website, known as Playpen, hosted large quantities of videos and still images of child sexual abuse as well as forums hosting discussions related to the hands-on sexual abuse of children.[70]

The FBI was able to verify the illegal activity and the location of the server, which was in Florida. The operation of Tor, however, made it impossible to identify the IP addresses—and thus physical locations—of perpetrators.[71] Beyond the important goal of eliminating and punishing the distribution of child sexual abuse materials, the FBI had reason to believe the identification of individual Playpen users might lead to the identification of victims of ongoing abuse.

Playpen prohibited the "cross-posting" of materials from other child pornography sites.[72] This means that, by virtue of posting, the user was certifying that he had individually created or commissioned the abuse material in question. In a significant number of instances, the perpetrator also identified the relationship to the victim through titles, descriptions, or selection of forum.[73] The site also had a written forum dedicated to recounting episodes of abuse, divided into fiction and nonfiction. The nonfiction forum housed detailed confessions of sexual abuse of minors, including accounts of ongoing abuse. Other postings offered or solicited advice on grooming victims. Still others provided a venue for users to encourage others to continue and escalate their sexual abuse of minor victims and advice on concealing those crimes.

To identify users, the FBI sought a warrant authorizing a network investigative technique (NIT).[74] The FBI seized the website and moved it to a government-controlled server located in the Eastern District of Virginia.[75] Federal officers then obtained a search warrant from a magistrate judge in that district to execute the NIT against any user who logged into the site.[76] Relying on an undisclosed exploitable flaw within Tor, the government was able to circumvent security features and deliver a payload of information to an activating computer that accessed particular pages hosting contraband within Playpen following login.[77] That payload surreptitiously caused the computer to transmit information back to the government computer, including an unmasked IP address.[78]

The FBI derived the computer's physical location from the unmasked IP address and then used that information to obtain search warrants within the individual jurisdictions.

The Playpen Warrant and Future Lawful Hacking Warrants

The Playpen cases raise a number of Fourth Amendment questions. Broadly, the controversies involve (1) whether the investigative technique qualified as a search within the meaning of the Fourth Amendment, (2) whether a magistrate judge had authority to issue a warrant under the existing Rule 41 of the Federal Rules of Criminal Procedure, and (3) whether the warrant satisfied constitutional requirements regarding probable cause and particularity.

On at least the first question, courts have reached generally broad agreement that the operation of this NIT qualified as a search of the target computer. The question rests on whether the nature of the information obtained—primarily, an Internet protocol address—voids the defendant's reasonable expectation of privacy. As a general matter, under the third-party doctrine, there is no reasonable expectation of privacy in an IP address, which is displayed to any number of third parties by virtue of its function.[79] When using Tor, a user's genuine IP address is shared with the first node, though it is disguised as it passes through intermediary nodes, and the intended purpose of Tor is to hide the true IP address from the ultimate destination.

In a small number of cases, the government has argued that because a Tor user shares his or her IP address with an initial third party, there is no longer any reasonable expectation of privacy in that information and, therefore, "the government's acquisition of the IP address did not constitute a search."[80] But courts have largely concluded—and some federal prosecutors have conceded—that the partially public nature of the IP address is not relevant when the government obtains the information directly from a defendant's computer. Explaining the prevailing rule, Fourth Amendment scholar Professor Orin Kerr notes[81] that the relevant fact is "how the government obtained the information, not whether it could have obtained the information some other way that would not be a search."[82]

Still, at least a few courts agreed with the government's assessment that there was no search with respect to the IP address.[83] The question of the expectation of privacy in masked IP addresses will be highly significant for the future of lawful hacking and illustrates some of the tensions at play as technological developments strain first principles of the Fourth Amendment.

It is well established that individuals have a reasonable expectation of privacy in their personal computers. It is similarly true that IP addresses are not considered private under the prevailing read of the third-party doctrine. Yet, if courts determine that a masked IP address does not confer some additional protection, at least with respect to obtaining it directly from the user's computer, it would seem that there is nothing an individual can do to reestablish reasonable expectations of privacy. The third-party doctrine is already under serious strain as technology produces more information that users either are unaware of or cannot avoid sharing with third-party providers. By pushing legal theories that render individuals effectively powerless to establish privacy online, the government may speed either the demise of the third-party doctrine in court or the drive toward relying on encryption and other methods to avoid sharing usable data with third parties at all. This means that, counterproductively, pursuing an overly aggressive legal strategy on IP anonymization may exacerbate the Going Dark problem generally.

The Fight over Rule 41

As discussed above, it would be logically problematic if using a masked IP not only failed to confer additional privacy rights but actually reduced reasonable privacy expectations by rendering a computer with a masked IP eligible to be searched without a warrant. Conversely, it would be an equally absurd result if individuals within the United States were permitted to use Tor and other anonymizing techniques to place themselves beyond the reach of any federal magistrate, effectively immunizing themselves from warrants.

The latter motivated recent changes to Rule 41 of the Federal Rules of Criminal Procedure,[84] which took effect December 1, 2016. Previously, Rule 41 included territorial venue provisions authorizing magistrate judges to issue warrants only within their districts, except in a set of narrowly defined circumstances. Because—prior to obtaining a warrant—authorities did not know the physical location of a computer using Tor or other anonymization services, it was unclear whether law enforcement could obtain such a warrant from *any* federal judge.

As of November 2016, judges in more than twenty-five federal districts had presided over matters relating to a Playpen prosecution. A primary issue in these cases was whether the warrant, obtained in the Eastern District of Virginia, violated Rule 41 when applied to computers outside that district. Although courts diverged significantly in their analyses and conclusions,[85] a majority of courts found that the warrant at least technically violated Rule 41 but relied on the good-faith exception in declining to suppress evidence.

The December 1 rule change effectively moots the issue for future investigations. Under the new Rule 41, a magistrate judge is authorized "to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information within or outside that district if: (A) the district where the media or information is located has been concealed through technological means."[86] The amendment is designed to authorize the issuance of precisely the kind of search warrant the FBI obtained in the Playpen operation.[87]

There was substantial opposition to the rule change, and the promulgation of the new language is unlikely to end the substantive debate. Critics purported to take issue with the process by which the Federal Rules are changed, describing the governing Rules Enabling Act as an "obscure bureaucratic process"[88] and claiming that the procedures circumvented congressional input. This is an inaccurate characterization.

Under the Rules Enabling Act,[89] Congress mandated a process by which subject matter–specific advisory committees propose rules to a standing committee, which in turn proposes changes to the Federal Rules to the Supreme Court. The Supreme Court then considers the proposals and annually promulgates new rules, which can be rejected or modified by an affirmative act of Congress. Playpen and Rule 41 demonstrate the need for this judicially driven process.

Because most courts relied on the good-faith exception—acknowledging a violation of Rule 41 but declining to suppress evidence obtained—absent a swift rule change, investigators would have been effectively unable to identify the physical locations of many individuals who consume and distribute child pornography and in many cases offer (from the safety of their masked IP addresses) detailed confessions of ongoing "hands-on" offenses against minor victims. The Playpen saga thus offers a rather compelling demonstration of why the act shifts the burden to Congress to block rules the judiciary has deemed necessary and proper.

Rule changes are intended to promote the use of warrants, in part by making warrants easier to obtain. But rulemaking cannot alter constitutional warrant requirements, nor does it deprive Congress of the power to impose additional statutory constraints. Following the rule change, we are now in the far more desirable situation of having a clear mechanism by which law enforcement can seek a warrant—subject to constitutional constraints—as opposed to the prior circumstances whereby law enforcement was unable to obtain a warrant even where it was clearly constitutionally permissible.

Constitutional and Policy Constraints under the New Rule 41(b)

The Rule 41 change merely provides for the technical venue procedures for obtaining a warrant. The warrant itself functions as the vehicle by which a neutral magistrate determines constitutional sufficiency. Although opposition to the Rule 41 change largely took the form of slippery-slope arguments, the highly unusual and serious features of child sexual exploitation offenses function to set an extremely high bar for these types of warrants.

The Constitutional Requirement of Particularity and Probable Cause

Putting aside those now-mooted issues resulting from violations of the former Rule 41, the Playpen warrant provides a useful example of the possibility of constitutional adequacy for large-scale lawful hacking warrants. One objection raised in the context of the Rule 41 change and also in the Playpen cases is whether the type of warrant at issue here satisfies the Fourth Amendment requirements of particularity and probable cause.

The Fourth Amendment mandates that "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."[90]

Probable Cause

Notably, there is little controversy over whether the Playpen warrant satisfied the requirement of probable cause. The warrant authorized the FBI to deploy the NIT against any individual who logged into the website with a username and password. In issuing the warrant, the magistrate judge determined that where an individual undertook the steps to seek out a hidden website, where such website unabashedly advertised itself as dedicated to child pornography, and where the individual undertook to create a username and password to access the site, the conditions for probable cause were met.

As with all anticipatory warrants, probable cause did not exist at the time of issuance but was instead triggered when certain conditions were satisfied as to each individual user. Notably, the FBI deployed the NIT more conservatively than authorized by the warrant, and the NIT deployed not at login but only when users accessed pages within the site which unequivocally announced themselves as hosting contraband child pornography.

Defense attorneys have challenged the warrant as defective on the grounds that probable cause did not exist at mere login because an individual might have been seeking only to access socially appalling, but nonetheless legal, fictional accounts of child sexual abuse. Separately, the defense has asserted that the conditions of the anticipatory warrant were

not met because the web page logo submitted with the warrant application had been changed—from depicting two prepubescent scantily clad females to depicting a single scantily clad prepubescent female—and the new image did not qualify as "lewd and lascivious." Courts rejected both arguments on the merits. The oral arguments and orders, however, demonstrate that courts are fully empowered to determine whether warrants that might authorize a significant number of searches nevertheless meet all constitutional requirements with respect to each individual defendant.

Particularity

The Particularity Clause promotes two objectives: (1) "to minimize the risk that officers executing search warrants will by mistake search a place other than the place intended by the magistrate" and (2) to ensure a showing of probable cause as "the lack of a more specific description will make it apparent that there has not been a sufficient showing to the magistrate that the described items are to be found in a particular place."[91] The particularity requirement does not depend on rigid formality, and not every vague or mistaken description of a place to be searched invalidates a warrant.[92]

Likewise, the Supreme Court has held that anticipatory search warrants—those "based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of crime will be located at a specific place"[93]—are constitutional. To obtain an anticipatory warrant, a magistrate must determine "(1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed."[94]

Internet privacy advocates suggest that the warrant must fail particularity because it authorizes the search of any user who logs into the site rather than describing particular users to be searched.[95] Notably, these advocates do not argue that there was not probable cause for each and every search. Rather, because "there were over 150,000 registered member accounts and over 1,500 daily visitors to the site,"[96] each of whom could be searched upon logging into the site, the warrant simply swept up too many people.

But this misses the point of particularity and indeed the point of the Fourth Amendment. As noted above, particularity is intended to prevent mistakes and as a backstop to ensure probable cause. In the Playpen cases, probable cause was clearly satisfied as to each and every user that logged on to the site and accessed the contraband material that triggered the NIT. Similarly, the idea that there would be a mistaken search because of an ill-defined location is far-fetched.

Admittedly, the notion that one anticipatory warrant might net one hundred or one hundred thousand people does seem to stress the particularity requirement. But the Playpen warrant demonstrates not only how constitutional requirements can be met for so-called watering-hole attacks but also how such warrants can be executed in a manner that is exceptionally strong with regards to constitutional sufficiency. One reason particularity is very strong in this case is because the NIT in question is deployed at the moment the person actually accesses contraband material. At that moment, the individual has completed an offense.

Probable cause and particularity are malleable, and mutually reinforcing standards and courts should focus on the underlying purposes of the requirements. Playpen presents an extraordinarily strong case of probable cause and particularity for every single person that is searched. Indeed, the warrant as applied in Playpen offers a *stronger* form of particularity than "all persons warrants" that authorize the search of everyone who enters a brothel or drug house, for instance.[97] In those cases, you don't actually know that someone has yet completed an offense. But in the Playpen case, the NIT was deployed only upon the completed crime of accessing the contraband image.[98]

This gives us a powerful limiting principle. Instead of indulging the slippery slope, we should recognize the incredibly rare, if not unique, strength of the case of accessing a contraband image, a unique type of offense.

Courts evaluate warrants on their face for constitutional requirements. But the interplay between the Playpen warrant as issued and as applied demonstrates that the near-unique nature of child sexual abuse images and websites is highly relevant. Probable cause is satisfied by the Playpen warrant because it is overwhelmingly likely—and not just possible—that anyone logging into a website featuring lewd and lascivious images of young children has the single purpose of accessing contraband or engaging in discussions related to the sexual abuse of children. The same can probably not be said for other forms of "dark" marketplaces, which typically host both contraband and legal items. For example, it is unlikely a similar warrant would satisfy both probable cause and particularity if applied to a Tor service that offered the sale of illegal drugs. First, if enough legal materials exist on the site, it would dramatically undercut probable cause at login. Second, merely clicking on a web page that purported to sell illicit drugs is not itself a criminal act. The criminal act would require a user to actually purchase or attempt to purchase illegal narcotics. This suggests that, outside of the child sexual abuse materials context, warrants involving these tools are more likely to be specifically tailored to deploy an NIT only from pages where strong evidence of criminality with respect to the individual users exists. This is the precise aim of the particularity

requirement: to ensure warrants authorize searches in a way that reduces the probability of mistake. There is a very low probability of mistake in deploying an NIT against an individual who logged into Playpen but had no intention of committing any kind of offense or offering evidence of offline crimes. In contexts where the probability of mistake is higher, particularity will require additional limitations such as listing targeted usernames or limiting the NIT search to deploy only from pages that announce extremely high probability of criminal conduct—for example, a completed order or payment transaction.

Beyond the pure constitutional analysis, the specific nature of child sexual exploitation offenses and the operational realities created by Going Dark invite the need for a paradigm shift with respect to investigations. A core criticism of the Rule 41 change—and of the Playpen warrant in particular—is an objection to the government being able to "obtain a single warrant to access and search thousands or millions of computers at once."[99] The name of legislation opposing the rule change itself refers to "mass hacking."[100] These objections mirror the broader trends in surveillance of moving away from less differentiated forms of collection—characterized as bulk, mass, or dragnet—and toward more targeted forms. Generally speaking, these trends are positive and reinforce important privacy principles. But the specific features of this form of crime suggest that an emphasis on numbers misses critical operational realities and misconstrues the constitutional requirements.

As technology moves to more sophisticated security and as default settings minimize user mistakes—a positive outcome for regular users but a missed opportunity against criminals—the opportunities to discover child sexual abusers and to rescue victims are fewer. Although image-based identification is useful, the most common method of identifying victims is through perpetrators. Tools relying on unknown vulnerabilities or temporary misconfigurations are highly perishable. For any Going Dark solution to be meaningful, when a window of opportunity presents for law enforcement to identify perpetrators, the police must be able to do so for as many offenders as possible. "Mass hacking" is better understood in this context as one mechanism to embrace the many benefits of information security technological developments, including heightened privacy protections, while minimizing the most intolerable costs.

Policy Constraints for Lawful Hacking as an Investigative Technique

The relevant constitutional requirements represent a floor; additional constraints on the use of lawful hacking for the investigation of child exploitation may be appropriate as a matter of executive policy or statute. For example, policy guidelines, similar to those for undercover operations, could govern lawful hacking that temporarily facilitates criminal

activity. Standards should be set to balance probable harms and benefits and to ensure criminal activity is facilitated only where strictly necessary to prevent ongoing harm.

Privacy advocates and defense attorneys have alleged that the FBI's decision to host a website distributing genuine child pornography for a period of two weeks rises to the level of shocking and egregious misconduct meriting suppression. Thus far, courts have disagreed and questioned the sincerity of these objections.[101] Still, the operation illustrates a policy choice. There are concrete, important goals served by preventing the transmission of these images, apart from the hands-on abuse involved in production. The FBI, however, had compelling reasons to believe that the identification of users of the site would lead to the identification and rescue of victims from immediate and ongoing harm. Here, and in at least one other case,[102] the FBI determined that the interests of identifying hands-on abusers and producers and of rescuing child victims outweighed the harms caused by temporarily facilitating the distribution of child sexual abuse materials.

To the extent there are genuine objections to the FBI determination, the matter is one for Justice Department policy. Such policies should ensure that benefits significantly outweigh the harm, and it would be wise to incorporate input from victim advocacy groups like NCMEC.

The Centrality (and Mixed Motivations) of the Disclosure Issue

The Playpen cases surface tensions over another issue central to the future of not only lawful hacking but also government surveillance generally: the government's obligation to publicly disclose vulnerabilities.

The Vulnerabilities Equities Process

When the government discovers a technical software or hardware vulnerability, it confronts a difficult policy choice: Should it disclose the vulnerability so that it can be patched, increasing cyber security generally but undercutting law enforcement's ability to investigate crimes and gather intelligence? To make the determination, the government weighs harm-against-harm in the classified interagency vulnerability equities process (VEP).[103]

Because of the Playpen operation and other high-profile government hacking cases, the VEP is under increased scrutiny.[104] Many critics agree with the basic premise that, although information security interests trump other security equities in the vast majority of cases, there are circumstances in which vulnerabilities should be retained and exploited for law enforcement or intelligence purposes. But they argue that the VEP is insufficiently

transparent to appropriately evaluate the equities. This is a fair criticism, and there are a number of thoughtful proposals for reforming the VEP to better achieve these goals.

A number of vocal detractors, however, are apparently animated by the belief that it is *never* proper for the government to withhold vulnerabilities. Because information security threats are so broadly diffuse and the integrity of information security so central to a great many civil liberties, this group opposes any process of genuine balancing, instead favoring near-constant disclosure.

Tor Vulnerabilities

One less extreme version of the latter view manifests around Tor specifically. Although activists might tolerate some limited government nondisclosure, Tor is deemed to be of such sacrosanct value that essentially no governmental interest is sufficiently compelling to warrant nondisclosure.

Those decrying the Playpen NIT almost certainly fall within some variant of this group. Indeed, if the Tor vulnerability in Playpen does not qualify for proper nondisclosure under VEP review, it is nearly impossible to conceive of one that would. There is an overwhelmingly compelling government interest at stake: the identification and rescue of children subject to ongoing sexual abuse. Although critics dismiss these claims as overstated, as a result of this investigation the FBI identified thirty-seven individuals who had committed actual, hands-on sexual abuse of children—ending the abuse for whatever multiple of minor individuals comprised their victims. More important, the FBI has rescued forty-nine identified children from ongoing abuse.[105]

The Interplay of Vulnerabilities Disclosure Policy and the Legal Questions in Playpen

One central legal question in the Playpen cases is whether the government should be compelled to disclose all of the NIT code to individual criminal defendants.[106] Here, the interests of activists and defendants briefly align. Both wish to force the so-called disclose-or-dismiss choice.

Activists who oppose government hacking in general, or object to the decision to exploit a Tor vulnerability in particular, recognize that compelled disclosure in the Playpen cases has significant policy consequences. In the immediate, if the "exploit" must be disclosed—even under a protective order—then the vulnerability is likely to be patched. This has the benefit of reducing risk to legitimate users of Tor, but it has the downside of preventing law enforcement's ongoing use of the vulnerability—in essence, this is an attempt to re-litigate the determination to not disclose, whether it was made through the VEP or otherwise.

In the long term, however, the precedent that the government is obligated to disclose these kinds of exploits will have substantial impacts on the feasibility of lawful hacking. Hacking tools are necessarily perishable; ordinary security updates or shifts to new types of technology continually render existing techniques obsolete. An obligation to disclose a vulnerability in court would further reduce this already short useful life span. Although some proponents advocate for law enforcement to temporarily exploit and then quickly disclose a vulnerability for patching, this is infeasible in practice and would significantly limit the efficacy of lawful hacking as a broader solution.[107]

The Playpen defendants, on the other hand, have noted that the government is unwilling to disclose the vulnerability, even if it means dismissing charges. If the defendant can successfully convince a judge to require disclosure, he can in effect win dismissal of charges—this is a new variant of what is known as graymail.[108] This disclose-or-dismiss method was successfully pioneered in a Playpen case in the Western District of Washington,[109] though the same judge reached the opposite conclusion in later cases.[110] Other defendants have quickly followed suit with mixed results.

Right to Discovery in a Criminal Case

To understand how the government finds itself with the disclose-or-dismiss dilemma, it is first critical to understand the rules governing discovery in criminal cases. The Supreme Court has long held that "there is no general constitutional right to discovery in a criminal case."[111] Instead, the right is by and large procedural, governed by Rule 16 of the Federal Rules of Criminal Procedure.[112] Rule 16 specifies information discoverable by criminal defendants, including documents and data "material to preparing the defense."[113]

Although the right is largely rule-based, "there are constitutional imperatives that cannot be disregarded even though there is no constitutional right to discovery."[114] Under *Brady v. Maryland,*[115] the government is constitutionally obligated to disclose evidence that is both "material" and "favorable" to a criminal defendant.[116] Disclosure of this exculpatory evidence is thought to be so central to a fair trial that its denial violates due process.[117]

Rule 16 governs the procedural right to discovery. In *Roviaro v. United States,*[118] the court examined the government's asserted privilege to withhold the identity of informants, noting that the "purpose of the privilege is the furtherance and protection of the public interest in effective law enforcement."[119] But the so-called law enforcement privilege is limited, and where the disclosure "is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way."[120] The court decidedly rejected any "fixed rule," opting instead for a balancing of "the public

interest in protecting the flow of information against the individual's right to prepare his defense" and "taking into consideration the crime charged, the possible defenses, the possible significance of the [evidence], and other relevant factors."[121] *Jencks v. United States,*[122] decided the same year as *Roviaro,* held that a "criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce, for the accused's inspection and for admission in evidence, relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at trial."[123] Thus, the government faces a choice: disclose the privileged information or dismiss the charges.

The touchstone of both a constitutional due process disclosure obligation and Rule 16 is materiality. Evidence is constitutionally material "only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."[124] "Reasonable probability" means "a probability sufficient to undermine confidence in the outcome."[125] But for the purposes of Rule 16, because the analysis must occur ex ante, the defendant must make a prima facie showing of materiality by providing "some indication that the pre-trial disclosure of the disputed evidence would enable defendant significantly to alter the quantum of proof in his or her favor."[126]

Disclose or Dismiss: Graymail Incentives and Determining Materiality

The incentives toward graymail and the challenges in determining materiality of highly technical evidence are starkly illustrated by the series of Playpen cases in the Western District of Washington. There, the same judge, ruling on identical legal questions related to the same warrant and NIT, reached opposite conclusions in two different orders relating to four defendants.

At issue is whether the defendants are entitled to see the "exploit" portion of the NIT. In both cases, the defense sought discovery of the computer code used to execute the NIT. The government agreed to provide the "payload" executed on the target's computer as well as the two-way network data exchanged between the target computer and the government-controlled computer as a result of the NIT.[127] The FBI attested that "the data stream from [the defendant's] computer is identical to the data" provided in discovery, that the data stream confirms no images were transmitted to or from the defendant's computer, and that once the NIT was completed, "nothing resided on [defendant's] computer that would allow the government (or some other user) to go back and further access that computer."[128]

Nevertheless, the defense asserted it was entitled to examine all the computer code involved in the NIT, including the code describing the exploit used to access the

defendant's computer. In essence, the government asserts that only code related to what occurred on the defendant's physical machine is relevant or material, whereas the defendants claim they are entitled to understand how the government accessed the machine to mount a fair defense.

In *Michaud,* Judge Robert Bryan sided with the defense and ordered that, if the government elects not to disclose the exploit, all evidence derived as a result of the NIT must be excluded. A number of months later, in a consolidated order on three other cases—*Tippens, Lesan,* and *Lorente*—he adopted the government's view.

The evolution of an individual judge between these cases illustrates one feature of lawful hacking that will undoubtedly arise again in the future: How can judges make legal determinations about the significance of computer code that they do not understand? It is important to note that this is not simply a matter of a judge changing his mind. For purposes of resolving similar issues in the future, the episode is better understood as the government failing to explain sufficiently the facts in the first set of cases—potentially risking a defendant evading justice—and sufficiently explaining them in the second. The question then becomes how to avoid the first situation (insufficient information) and replicate the second (sufficient information), regardless of the specific outcome.

It is commonplace for the judiciary to lack subject matter expertise in scientific or technical evidence presented in their courts. For example, we don't expect judges to possess prior knowledge of the science behind carbon emissions in ruling on related environmental regulations. Typically, the adversarial system produces a battle of experts, offering various interpretations of the relevant facts, which a judge (or jury) can weigh for credibility and relevance before reaching an ultimate conclusion. Computer code is no different.

What is novel here is the combination of highly technical evidence *and* secrecy. In both *Michaud* and *Tippens,* Judge Bryan concluded that the government had properly asserted privilege and that the exploit in question could not be safely disclosed to the defense, even under a protective order. The application of the Classified Information Procedures Act (CIPA) or law enforcement privilege eliminates the adversarial element. If the defense experts cannot see a particular piece of evidence, the judge is forced to rely on the defense's assertions as to what such evidence *might* contain and the government's assertions as to what such evidence *actually does* contain. Unlike other applications of CIPA, which involve written facts that a judge can independently evaluate, it is highly unlikely that a member of the judiciary would be qualified to make such an evaluation here. The ruling in *Michaud* demonstrates the perils of graymail and assessing materiality in the context of lawful hacking.

Indisputably, the exploit code provides some additional information about the function of an NIT. For information over which the government has asserted law enforcement privilege, however, the defense is entitled only to that which is "material" to its case. The FBI and defense offered a battle of experts as to the potential relevance of the exploit code. The defense asserted the exploit code was needed to make a number of broad determinations, without articulating how those determinations might relate to the defense's theory of the case. The government rebutted those claims and offered somewhat broad metaphors to persuade the court: "In layman's terms an 'exploit' could be thought of as a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key" and that the code itself was immaterial because "knowing how someone entered the front door provides no information about what someone did after entering the house."[129]

Faced with dueling technical expert testimony, the court was unwilling to defer to the FBI's assertions. The judge was candid in oral arguments, saying, "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."[130]

Absent the ability to make independent assessments as to the validity of the dueling technical theories, the judge concluded that the exploit code was material and therefore must be disclosed or the evidence excluded. But, critically, the ruling indicates Judge Bryan never reached a conclusion on the technical merits regarding whether the exploit code is material to the defense's specific theory of the case. Instead, he substituted a broader determination that the code seems like an important issue: in ordering discovery, the court stated that it was "satisfied that the defense has shown materiality . . . I don't need to discuss that in depth, in my view. I think the papers speak for themselves."[131]

The problem is that complexity and materiality are not actually the same. In *Michaud,* the court essentially defers to the defense experts' declarations as to the importance of the exploit. Following *Michaud,* independent public analysis of the defense declarations, including by Mozilla, which writes the code at issue, determined that although there are a number of scenarios in which the exploit code might offer additional information, there is only one scenario in which such information would also be relevant in any way to an actual defense: if the FBI had deliberately programmed the NIT to exceed the scope of the warrants and then lied to the judge.[132] In *Tippens, t*he court returned to the declarations with a critical eye and, in evaluating those same claims as related to the defendants' specific claims at trial, found the exploit was not material. In short, the

government did a better job at explaining the technical materials in the second set of cases than it did in the first.

What occurred in the early Playpen cases is a clear manifestation of graymail. The Department of Justice acknowledged that the tool in question was too sensitive to disclose. As soon as it became clear the government would elect dismissal over disclosure—and the successful suppression motion in *Michaud*—a rash of defendants caught in the Playpen sting rushed to make motions to compel discovery of the exploit code. The problem is that all defendants are incentivized to claim materiality, even if they are well aware the exploit is not material to their factual situation.

The perverse graymail incentive appears not where there is a determination that the information is actually material, but where it is too complex for the judge to conclusively determine its non-materiality. Where defendants' substantive rights are at stake, courts err toward disclosure. A long-term solution is needed because, inevitably, a future case will present a proper question of materiality; some future defendant really will need to see the exploit to mount a fair defense. The challenge is empowering the judiciary to recognize those cases of true materiality, without the "false positive" that occurred in *Michaud*.

Ensuring that Disclose or Dismiss Doesn't Undermine Lawful Hacking

The highly technical and highly sensitive nature of exploit source code used in NITs risks the over-disclosure of information that imperils core law enforcement functions without meaningfully advancing defendants' legitimate interests. As law enforcement tools become increasingly complex and as Going Dark drives additional need for both hacking tools and secrecy, the problem is likely to worsen. A new mechanism is needed to facilitate the judiciary making determinations regarding the materiality of highly technical information in the context of an exceedingly high need for secrecy.

Other courts have yet to consider the questions regarding law enforcement privilege and the materiality of the exploit code. The eventual majority view on the matter—either as to the Playpen NIT in particular or obligation to disclose exploits in general—is still unclear. If a number of courts follow *Michaud,* however, potentially serious negative outcomes could result. It could create incentives for law enforcement to not invest in developing hacking tools where the limited useful life spans cannot justify high costs. Alternatively, such precedent could incentivize law enforcement to assert classification rationales in lieu of law enforcement privilege or attempt to use parallel construction to circumvent the disclosure risks.

The solution to the graymail issue in the context of classified national security secrets was legislation. *Roviaro* mandated balancing executive interest in secrecy with a defendant's right to a fair trial. In response, Congress passed the Classified Information Procedures Act (CIPA), which provided procedures for handling discovery of classified information in espionage and terrorism prosecutions.

If lawful hacking is going to be a meaningful solution to Going Dark, Congress may need to develop a legislative framework for procedures surrounding highly technical, privileged law enforcement information. Such procedures could not alter the substantive constitutional rights of defendants but would ensure that the disclose-or-dismiss dilemma arises only where the tool is, in fact, material to the defense.

A new framework would need to account for threshold determinations regarding the assertion of privilege and whether information properly falls within the scope of privilege. Procedures could also modify the rule to address whether alternative methods or summary information can satisfy the defendant's basic inquiry. In essence, the intention of such legislation is not to eliminate the possibility of the disclose-or-dismiss dilemma but instead to ensure it arises only where constitutionally or otherwise appropriate and not as a Hail Mary litigation strategy.

International Dimensions of Going Dark and Combating Child Sexual Abuse

Child sexual exploitation is a distinctly global law enforcement challenge, and the international features add significant operational and legal complexity. Data are increasingly likely to be stored both in multiple jurisdictions and in jurisdictions outside the primary investigating body. Both offenders and victims are located all over the world. And manifestations of the Going Dark problem specifically challenge traditional methods of establishing primary jurisdiction and respecting national sovereignty when executing computer searches.

Jurisdiction and Cross-Border Data Requests

Not only are online child pornography crimes "borderless" in nature, but it is now increasingly likely that evidence will be located within multiple jurisdictions.[133] Because of the global scope and inherently cross-border nature of the crime, international law enforcement cooperation and standards are critical. Nations cooperate formally through bilateral and multilateral mutual legal assistance treaties (MLATs) and informally through mechanisms like Article 35 of the Council of Europe Cybercrime Convention (known informally as the "Budapest Convention"). Article 35 requires signatories to "designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance" of investigations.[134]

The formal mechanisms are utterly inadequate, with average response times of nearly 150 days.[135] The informal mechanisms reportedly yield responses to 90 percent of requests within one month.[136]

These time frames are not responsive to the investigative requirements of child sexual exploitation offenses. Although prosecution timelines can support delays in obtaining relevant data evidence located in other countries, time is of the essence when attempting to identify and rescue victims. Although a number of proposals currently exist for reforming the MLAT process, little progress has been made in practice, and there is insufficient urgency in implementing solutions.

Additionally, some forms of child exploitation crimes—the transmission and receipt of child sexual abuse material—can take place entirely online. Unlike international trafficking in other forms of contraband, such as narcotics, there is no need to interact with physical borders or postal systems. Therefore, many mechanisms designed to control the international transmission of contraband are inapplicable.

International Cooperation

Joint operations and international organizations are one way countries address the global dimensions of crime. Operations coordinated by Interpol have netted notable successes. The outcomes of those operations serve to highlight further the international complexity and compelling interests of individual nations—for example, a single operation led to sixty arrests in fourteen countries and to the identification of fourteen underage victims in Spain and two in Colombia.[137] Europol has also undertaken ambitious internationally coordinated efforts, including one large-scale effort involving law enforcement representatives from thirteen countries investigating more than two hundred child pornography websites operating on Tor.[138] Coordination also occurs directly among countries at the national level. A joint investigation among authorities in Australia, Canada, and the United States led to the arrest of 348 individuals in the United States and twenty individuals in Canada with over one hundred minor victims identified and rescued in those countries alone.[139]

Certainly, internationally coordinated efforts will be one important avenue to address the problem of the sexual exploitation of children and exchange of child sexual abuse images. But such operations are complex and expensive and can hope only to supplement primarily domestic efforts.

Going Dark Challenges to Identifying Jurisdiction and Sovereignty

Now and moving forward, international cooperation more commonly bookends primarily domestic investigations: foreign partners alert law enforcement agencies to the existence of a website or victim likely located within their jurisdiction; the law enforcement agencies execute an investigation pursuant to domestic law and then share evidence of crimes or victims outside the jurisdiction with the relevant authorities. The Playpen case is a textbook example. Foreign partners notified US authorities of the existence of the site in the United States. The Playpen operation revealed IP addresses outside the United States, and information was shared with those countries.

But features of Going Dark actually prevent the identification of jurisdiction. First, various forms of encryption and other technologies and trends block access to images and video. Often, the examination of images themselves is used to establish probable jurisdiction. One of the most important methods of victim identification, for example, depends on content access. Groups of international investigators sit down together with pictures and attempt to identify the probable jurisdiction by examining the backgrounds. Investigators look at street signs, bridges, store names printed on shopping bags for something they recognize; sometimes it comes down to a vague feeling that the scenery reminds them of a particular country. Because a single offender often possesses materials produced in a number of countries, access to images is critical to the identification of appropriate jurisdiction.

Second, as the Playpen case illustrates, IP anonymization tools can make it impossible to know the physical location of a computer. Because offender communities typically involve both members and victims from multiple countries, law enforcement operations like Playpen are more likely than not to involve computers located in a foreign country and outside the jurisdiction of the investigating agency.

Current international and US frameworks do not adequately account for this situation. The Department of Justice manual on obtaining electronic evidence in criminal investigations contains detailed procedures for obtaining evidence located abroad, for example, but its advice is entirely country-specific and dependent on advanced knowledge of where the evidence is located.[140] The manual advises that when "United States law enforcement inadvertently accesses a computer located in another country, [the Computer Crime and Intellectual Property Section of the Criminal Division], [the Office of International Affairs], or another appropriate authority should be consulted immediately, as issues such as sovereignty and comity may be implicated."[141]

The Playpen case highlights how existing paradigms of international cooperation and law enforcement guidance fail to account for a situation in which specific advance knowledge of where the evidence will be found is lacking and in which the search cannot reasonably be characterized as "inadvertent." Investigators executing a warrant like that in the Playpen cases know in advance that their searches are extremely likely to occur in foreign jurisdictions but have no way of knowing which ones.

Although there is no prohibition in US law against obtaining evidence from abroad, typically the government pursues the cooperation of foreign law enforcement on matters relating to jurisdiction. It is possible that a foreign government would view the execution of an NIT on a computer residing in its territory as a violation of sovereignty.[142] One open question is how the United States might establish reciprocal norms governing the use of remote "searches" of computers for which the location is unknown.

Child Exploitation and Offense-Based Solutions

On the international challenges, this paper will conclude where it began: by suggesting there is significant utility in grounding broader conversations regarding data and technology in the specific challenge of combating child sexual exploitation online.

Just as the debate over Going Dark in the United States is complicated by various equities, the international conversation is taking place amid substantial shifts. For example, opposition to MLAT reform often implicates divergent views on privacy, data protection, legal protections, definitions of criminal conduct, and basic human rights. In this sense, the small areas in which most countries can agree fall victim to the larger unresolved problems. For that reason, considering the urgency of the child sexual abuse problem and the intractable nature of the broader disagreements, it may be sensible to shift MLAT reform and similar efforts away from establishing human rights frameworks and toward offense-specific and evidence-based standards. The vast majority of countries criminalize child pornography as a general offense.[143] Agreements to facilitate more smoothly data access to investigate these crimes—particularly when there is some showing that a minor child within the jurisdiction faces the risk of immediate harm—not only have potential to relieve immediate pressures but also might offer models that could be generalized to other very serious crimes.

The same may be true for developing international norms regarding inadvertent, but not unwitting, violations of sovereignty in investigating the locations of anonymized computers. Reciprocal acceptability is a touchstone of international norms; we must be willing to accept other countries' rights to exercise the same methods against computers within the United States. Clearly, permitting foreign governments to perform remotely

computer searches in the United States would not be acceptable, nor would the United States assert the right to do so abroad in violation of foreign domestic laws. It may be possible, however, to gain broad support for limited norms permitting the use of investigative techniques for commonly defined crimes involving the sexual abuse of minors for the purposes of obtaining only the information necessary to make a predicate determination on jurisdiction.

The enormous complexities of Going Dark, both domestically and internationally, will require years of robust debate and careful deliberation. Ever-evolving technologies are a moving target, and we may never reach a stable long-term understanding as laws and institutions adapt. But the answer to evolving uncertainty cannot be to remain frozen, endlessly replaying our ideological commitments at home and abroad.

There are simply too many children still in darkness, waiting.

NOTES

1 Going Dark refers to the phenomenon by which the government has a legal right to access data but lacks the technical or practical ability to do so. In 2011, FBI General Counsel Valerie Caproni used the term to describe "a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications." Valerie Caproni, statement before the House Judiciary Committee, Subcommittee on Crime, Terrorism and Homeland Security, February 17, 2011.

2 International bodies, including the United Nations, call for the use of the term "child sexual abuse materials." These groups caution that "child pornography" insufficiently distinguishes consensual adult pornographic materials from acts of violence against children. While sensitive to those concerns, because "child pornography" is a legal term of art in the United States and is defined in statute, the terms will be used interchangeably here.

3 Darkness to Light: End Child Sexual Abuse, "Child Sexual Abuse Statistics," www.d2l.org/atf/cf/%7B64AF78C4-5EB8-45AA-BC28-F7EE2B581919%7D/all_statistics_20150619.pdf.

4 Ibid.

5 Ibid.

6 US Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction,* April 2016, 8, www.justice.gov/psc/file/842411/download.

7 Ibid.

8 US Department of Justice, *The National Strategy for Child Exploitation Prevention and Interdiction,* August 2010, 11, www.justice.gov/psc/docs/natstrategyreport.pdf.

9 Thorn (Digital Defenders of Children), "Child Pornography and Abuse Statistics," www.wearethorn.org/child-pornography-and-abuse-statistics/.

10 *National Strategy* 2016, 74.

11 Ibid.

12 Ibid., 2.

13 Ibid., 3.

14 Ibid., 24.

15 Ibid., 3.

16 Ibid.

17 Ibid.

18 Ibid., 4.

19 Ibid. From 2005 through 2009, US Attorneys prosecuted 8,352 total child pornography cases. *National Strategy* 2010, 11.

20 *National Strategy* 2010, 8.

21 In 2001, 261,653 sites were identified, and in 2004 that number grew to 480,000 sites. *National Strategy* 2010, 15, citing United Nations, "Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, Najat M'jid Maalla," July 13, 2009, A/HRC/12/23.

22 Ibid.

23 *National Strategy* 2010, 15–16.

24 *National Strategy* 2016, 72.

25 *National Strategy* 2010, 22.

26 *National Strategy* 2016, 143.

27 Ibid.

28 Ibid., 72.

29 Ibid., 73.

30 *National Strategy* 2010, 19.

31 *National Strategy* 2016, 73.

32 Ibid., 143.

33 *National Strategy* 2010, 22.

34 Ibid. Sixty-three percent of 2010 respondents reported increased violence toward child pornography victims, 42 percent more bondage, 38 percent more sadism and masochism, and 15 percent more bestiality.

35 Ibid.

36 Jim Bronskill, "Canadian Police Lack Resources to Keep Up with Online Child Pornography, Federal Memo Warns," *Toronto Star,* July 4, 2016, www.thestar.com/news/canada/2016/07/04/canadian-police-lack-resources-to-keep-up-with-online-child-pornography-federal-memo-warns.html.

37 Eric Holder Jr., speech at the National Strategy Conference on Combating Child Exploitation in San Jose, California, May 19, 2011, www.justice.gov/criminal-ceos/child-pornography.

38 *National Strategy* 2016, 80.

39 Ibid.

40 Ibid., 143.

41 Ibid. More than 36 percent reported a significant increase in the use of anonymization tools, services, and networks, and more than 30 percent reported a significant increase in the use of encryption.

42 For example, a Philadelphia police officer suspected of possessing child pornography is currently in jail on contempt charges for refusing to decrypt password-protected hard drives. David Kravets, "Child Porn Suspect Jailed Indefinitely for Refusing to Decrypt Hard Drives," *Ars Technica,* April 27, 2016, http://arstechnica.com/tech-policy/2016/04/child-porn-suspect-jailed-for-7-months-for-refusing-to-decrypt-hard-drives/.

43 *National Strategy* 2016, 9.

44 Kristin Finklea, "Dark Web," Congressional Research Service report, July 7, 2015, 4, www.fas.org/sgp/crs/misc/R44101.pdf.

45 Ibid.

46 Federal law prohibits the production, distribution, reception, or possession of an image of child pornography using or affecting any means or facility of interstate or foreign commerce. See 18 USC §§ 2251, 2252, 2252A.

47 *National Strategy* 2016, 73. "FBI's analysis of one particularly egregious website on Tor found that it hosted approximately 1.3 million images depicting children subjected to violent sexual abuse. Analysis of these specific files identified at least 73 new victims previously unknown to law enforcement." Ibid., 74.

48 Finklea, "Dark Web," 9.

49 Ibid., 6.

50 *National Strategy* 2016, 36.

51 Ibid., 74.

52 *National Strategy* 2010, 3.

53 Ibid., 23–24.

54 Benjamin Wittes, Clara Spera, Cody Poplin, and Quinta Jurecic, "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault," Brookings Institution, May 11, 2016, www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

55 *National Strategy* 2010, 24.

56 Ibid., 23.

57 One 2009 survey of US Internet crime investigators found that 61 percent reported cases being detrimentally affected because data were not retained, and 47 percent reported that they had had to end an investigation because data were not retained. *National Strategy* 2010, 23n40.

58 Ibid. Efforts to create such laws would surely meet strong opposition on privacy grounds; similar efforts have been struck down by European courts.

59 *National Strategy* 2016, 80.

60 Ibid., 16.

61 Ibid., 91.

62 Ibid., 74. The same study "estimated 840,000 worldwide unique installations per month of P2P programs sharing child pornography," which indicates a significant increase of new devices confirmed to be trading child pornography.

63 One Thorn study suggests more than 30 percent of searches in the eDonkey P2P network are related to child sexual abuse content. Thorn, "Statistics."

64 *National Strategy* 2016, 92.

65 *National Strategy* 2010, 24.

66 See Steven Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, "Lawful Hacking: Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property* 12, no. 1 (2014): 5.

67 Susan Hennessey, "Lawful Hacking and the Case for a Strategic Approach to 'Going Dark,' " Brookings Institution, October 7, 2016, www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/.

68 *National Strategy* 2010, 20–21.

69 Leslie R. Caldwell, "Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation," US Department of Justice (blog), November 21, 2016, www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

70 *United States v. Michaud,* order denying defendant's motion to suppress evidence, 3:15-cr-05351-RJB (Western District of Washington 2015), 2.

71 *Michaud,* order denying motion to suppress, 3.

72 Ibid., 2.

73 For example, in one video described in federal affidavits the user identifies the victim of penetrative rape as a nine-year-old niece. Additionally, forums dedicated to depictions of incest also identified victims as immediate family members. Affidavit of Daniel Alfin, *Michaud.*

74 *Michaud,* order denying motion to suppress, 3–7.

75 Ibid.

76 Ibid.

77 Ibid., 3.

78 Ibid., 3–5.

79 *United States v. Caira,* 833 F.3d 803, 806 (7th Cir. 2016), http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2016/D08-17/C:14-1003:J:Williams:aut:T:fnOp:N:1812349:S:0.

80 *United States v. Lemus,* government's opposition to defendant's motion to suppress evidence, 8–12.

81 Orin Kerr, "Remotely Accessing an IP Address Inside a Target Computer is a Search," *Washington Post,* October 7, 2016, www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/07/remotely-accessing-an-ip-address-inside-a-target-computer-is-a-search.

82 Ibid. By Kerr's analogy, the IP address as obtained from the defendant's computer is similar to a copy of leftover birthday invitations stored in a kitchen drawer; the mere fact that hundreds of identical invitations have been sent and could be obtained without a warrant does not mean police obtaining the information directly from one's home is not a search under the Fourth Amendment.

83 See *United States v. Werdene,* memorandum, 2:15-cr-00434-GJP, Dkt. 33; *United States v. Darby,* order and opinion, 2:16-cr-000036-RGD-DEM, Dkt. 31.

84 Federal Rules of Criminal Procedure, 41.

85 See *Michaud,* order denying motion to suppress, 12 (noting that the warrant violated "the letter, but not the spirit, of Rule 41(b)"); *United States v. Darby,* No. 2:16cr36, 2016 US Dist. LEXIS 74960 (Eastern District of Virginia, June 3, 2016) (concluding that because the defendant's computer was unluckily in the Eastern District of Virginia, Rule 41 was not violated); *United States v. Michaud* (concluding that although Rule 41 was violated, it was a technical violation that did not require suppression of the evidence obtained and that law

enforcement had acted in good faith); *United States v. Levin,* No. 15-10271-WGY, 2016 US Dist. LEXIS 52907 (District of Massachusetts, April 20, 2016) (concluding that the warrant was void ab initio due to the Rule 41 violation and fully suppressing the evidence obtained).

86 Federal Rules of Criminal Procedure, 41(b)(6)(A).

87 The new provision 41(b)(6)(B) is designed to eliminate challenges posed by investigations into botnets.

88 Senator Ron Wyden (D-OR), "Wyden: Congress Must Reject Sprawling Expansion of Government Surveillance," news release, April 28, 2016, www.wyden.senate.gov/news/press-releases/wyden-congress-must-reject-sprawling-expansion-of-government-surveillance.

89 28 USC § 2072.

90 US Constitution, Fourth Amendment.

91 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment,* 5th ed. (St. Paul, MN: West, 2012).

92 Ibid.

93 *United States v. Grubbs,* 547 US 90, 94 (2006) (quoting LaFave, *Search and Seizure,* 4th ed., 2004).

94 Ibid., 96.

95 Brief of amicus curiae, Electronic Frontier Foundation, *United States v. Matish,* 4:16-cr-16 (Eastern District of Virginia, May 9, 2016), www.eff.org/files/2016/06/17/ourbrief-filed.pdf.

96 Ibid., 13.

97 As the EFF brief correctly notes, jurisdictions differ as to treatment of "all persons warrants." Brief of amicus curiae, Electronic Frontier Foundation, 16. The point is simply that the argument that all persons warrants "contain greater particularity" than the Playpen warrant does not hold up when one focuses on the fact that the search in Playpen occurs only at the point at which there is extremely powerful probable cause—indeed, a complete offense—as to the particular individual searched.

98 This is not to say the warrant was invalid on its face or as applied to users at login. Even at login, the specific nature of child sexual abuse materials is a highly relevant feature of the probable cause analysis.

99 Wyden, "Government Surveillance," 89.

100 S. 2952, Stopping Mass Hacking Act.

101 In an oral ruling on the issue, the trial court in *Michaud* stated, "I am not shocked by this. I do not find it outrageous." *Michaud,* hearing transcript, 42. However, the same judge adopted a potentially contrary position regarding the nature of the government's conduct. *United States v. Tippens, et al.,* consolidated order on defendant's motion to dismiss indictments, Western District of Washington, 3:16-cr-05110-RJB, Dkt 106.

102 The FBI conducted a similar sting operation that involved hosting child sexual abuse material that was disclosed in a Nebraska prosecution, *United States v. Cottom,* No. 8:13CR108, 2013 US Dist. LEXIS 174801 (District of Nebraska, December 12, 2013).

103 For helpful background on the vulnerability equities process, see Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process," discussion paper 2016-04, Cyber Security Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, June 2016, http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

104 This section is adapted from Susan Hennessey, "Vulnerabilities Equities Reform That Makes Everyone (And No One) Happy," *Lawfare* (blog), www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy.

105 Leslie R. Caldwell, "Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation," US Department of Justice (blog), November 21, 2016, www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

106 Susan Hennessey and Nicholas Weaver, "A Judicial Framework for Evaluating Network Investigative Techniques," *Lawfare* (blog), July 28, 2016, www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques.

107 Hennessey, "Lawful Hacking," 67.

108 Graymail originally manifest in the context of national security prosecutions—espionage and terrorism—where a criminal defendant "creates a 'disclose or dismiss' dilemma," forcing the government to "choose between going forward with the prosecution, thereby compromising the classified material, or safeguarding the material but dropping the prosecution." Arjun Chandran, "The Classified Information Procedures Act in the Age of Terrorism: Remodeling CIPA in an Offense-Specific Manner," *Duke Law Journal* 64:1411, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3807&context=dlj (citing graymail legislation: Hearings Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence, 96th Cong., 1st Sess. 1 (1979) (statement of Rep. Morgan Murphy, chairman of the subcommittee)).

109 *United States v. Michaud,* order denying dismissal and excluding evidence, 3:15-cr-05351RJB, Dkt. 212.

110 *United States v. Tippens,* consolidated order.

111 *Weatherford v. Bursey,* 429 US 545, 559 (1977).

112 Federal Rules of Criminal Procedure, 16.

113 Federal Rules of Criminal Procedure, 16(a)(1)(E)(i), (F)(iii).

114 Charles Alan Wright, Andrew D. Leipold, Peter J. Henning, and Sarah N. Welling, *Federal Practice and Procedure: Criminal Subset,* 4th ed., 2016 supplement, §256 (Eagan, MN: Thomson West, 2007).

115 373 US 83 (1963).

116 Ibid., 87. A classic example of a so-called *Brady* violation occurs when the prosecution withholds a statement by a co-defendant exculpating the defendant of certain conduct.

117 See *United States v. Bagley,* 473 US 667, 675 (1985). "[The *Brady* rule's] purpose is . . . to ensure that a miscarriage of justice does not occur. Thus, the prosecutor is not required to deliver his entire file to defense counsel, but only to disclose evidence favorable to the accused that, if suppressed, would deprive the defendant of a fair trial" (opinion of Supreme Court Justice Harry Blackmun).

118 353 US 53 (1957).

119 Ibid., 59.

120 Ibid., 60–61.

121 Ibid., 62.

122 353 US 657 (1957).

123 Ibid., 672.

124 *United States v. Bagley,* 473 US 667 (quoting *Strickland v. Washington,* 466 US 668, 694 n.13 (1984)).

125 Ibid.

126 Wright, *Federal Practice and Procedure,* §254.

127 *United States v. Michaud,* Daniel Alfin declaration, 2.

128 Ibid., 2–3.

129 Ibid., 3.

130 *United States v. Michaud,* 3:15-cr-05351-RJB, order on procedural history and case status in advance of May 25, 2016, hearing, 2.

131 Ibid.

132 "[Mozilla's] analysis regarding the technical arguments in these cases is largely consistent with Nick Weaver and Susan Hennessey's conclusions; that is, the information disclosed by the FBI is probably sufficient to determine the authenticity of evidence collected without additional disclosures regarding the vulnerability to the defendant." Marshall Erwin and Urmika Shah, "Hanging Internet Users Out to Dry," *Lawfare* (blog), August 12, 2016, www.lawfareblog.com/hanging-internet-users-out-dry.

133 *National Strategy* 2016, 16.

134 Council of Europe, "Convention on Cybercrime," article 35, www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

135 United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime," draft of February 2013, 205, www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

136 Ibid., 214.

137 "19 Arrested in Spain for Child Pornography," *Business Standard,* July 4, 2016, www.business-standard.com/article/news-ians/19-arrested-in-spain-for-child-pornography-116070400818_1.html.

138 According to DOJ, "The impact of this complex, technically sophisticated, multi-national criminal investigative effort was unparalleled: more than 200 child sexual exploitation websites taken offline, along with hundreds of other sites sponsoring or facilitating criminal activity; the activities of tens of thousands of online child pornographers disrupted; over four million images and videos of child sexual abuse seized, including more than 100 previously unknown series of child abuse images and new images from more than 50 existing series; and dozens of offenders identified and prosecuted throughout the world. The case also resulted in the largest seizure of virtual currency up to that time and the discovery of 120 previously unknown victims of child sexual exploitation." *National Strategy* 2016, 16–17.

139 Ibid., 25–26. In 2012, as part of Operation Protego, Immigrations and Customs Enforcement's Homeland Security Investigations, in cooperation with law enforcement in Australia and Canada, investigated a "foreign based image-hosting website." The site hosted legal adult pornography but also became a location to trade child sexual abuse material. Special agents and analysis sifted through users' records to identify targets. One thousand leads were distributed worldwide, resulting in 348 individuals in the United States and twenty individuals in Canada being arrested. More than one hundred minor victims were identified and rescued in North America: eighty-nine in the United States and sixteen in Canada.

140 Department of Justice, Office of Legal Education, *OLE Litigation Series: Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations,* 56–59.

141 Ibid., 58.

142 Department of Justice, US Attorney's Manual, Criminal Resource Manual, §267–68, "Obtaining Evidence Abroad—General Considerations," www.justice.gov/usam/criminal-resource-manual-267-obtaining-evidence-abroad-general-considerations.

143 UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime," 100.

The preferred citation for this publication is: https://lawfareblog.com/elephant-room-addressing-child-exploitation-and-going-dark

About the Author

SUSAN HENNESSEY

Susan Hennessey is Managing Editor of Lawfare and General Counsel of the Lawfare Institute. She is a Brookings Fellow in National Security Law. Prior to joining Brookings, Ms. Hennessey was an attorney in the Office of General Counsel of the National Security Agency. She is a graduate of Harvard Law School and the University of California, Los Angeles.

Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200