HONEYPOTS: NOT FOR WINNIE THE POOH BUT FOR WINNIE THE PEDO

—

LAW ENFORCEMENT'S LAWFUL USE OF TECHNOLOGY TO CATCH PERPETRATORS AND HELP VICTIMS OF CHILD EXPLOITATION ON THE DARK WEB

Whitney J. Gregory[*]

Cruelty, like every other vice, requires no motive outside itself—it only requires opportunity.[1]

INTRODUCTION

Lawyers, doctors, teachers, politicians, and Hollywood stars—what do they all have in common? Smarts? Success? Wealth? Respect in their communities? Demonstrating the terrible divergence between appearance and reality, some members of these professions are also frequent customers and producers of child pornography.

Contrary to what some may assume, child pornographers are not just antisocial, out-of-work, reclusive basement dwellers. They may be people you would least expect.[2] Take, for instance, the teen heartthrob Mark Salling, who starred on Fox's hit show *Glee* as handsome bad-boy Puck from 2009 to 2015. Twenty-fifteen was also the year Salling was arrested and charged

---

[*] Antonin Scalia Law School at George Mason University, J.D. Candidate, May 2019; Articles Editor, *George Mason Law Review*, 2018–19. This Comment is dedicated to the memory of my grandfather Guido A. Ianiero.

[1] George Eliot, *Janet's Repentance*, *in* SCENES OF CLERICAL LIFE 102, 146 (Harper & Bros. 1858).

[2] Judges have described child pornography defendants as seemingly ordinary, even upstanding, men (and a few women). "The defendants' professional careers [are] often highlighted, including Air Force Captain, physician, trust specialist, and teacher." Melissa Hamilton, *The Efficacy of Severe Child Pornography Sentencing: Empirical Validity or Political Rhetoric?*, 22 STAN. L. & POL'Y REV. 545, 562 (2011) (footnotes omitted) (citing such cases, however, for a totally different proposition from that which is advocated in this Comment); *see also* United States v. Goff, 501 F.3d 250, 251, 253 (3d Cir. 2007). In vacating a below-Guidelines sentence as excessively lenient, the Third Circuit criticized the district court for having weighed heavily the fact that the fifty-four-year-old defendant led a "law-abiding and exemplary life." Underscoring that appearances lie, the Third Circuit stated, "For more than thirty years, [the defendant] was employed at a private elementary school . . . . Over time, he became a trusted and influential member of the school community. He was the president of his college alumni association . . . . He was, to all appearances, a respectable, middle-aged man leading a decent, law abiding life." *Id.*

with possession of child pornography.[3] His seized laptop and thumb drives contained over 50,000 images and videos of child pornography and child erotica. The content depicted sadistic abuse of children as young as two years old—toddlers not old enough for kindergarten.[4]

Court documents revealed that Salling knowingly downloaded his trove of child pornography between April and December 2015.[5] Not only is it frightening that he amassed so much child pornography in such little time, but it is equally frightening that it took him so long to get caught. The Dark Web (basically the "underground" part of the Internet) was his cloak—which explains how he was able to quickly stockpile child pornography and yet remain undetected. Salling hid his crime with software that masked his Internet Protocol ("IP") address.[6] However, he unmasked himself when he bizarrely showed some of these images to a woman in the context of their physical relationship.[7] She reported him to the authorities.

Having played a high school student on screen, the real life thirty-five-year-old Salling was banned from school yards.[8] In addition to serving jail time, the former star was ordered to pay at least $50,000 in restitution to each victim who requested it.[9]

The Salling saga brings up a variety of issues: the plague of child pornography, how technology has profoundly exacerbated this viral crime, and complications with victim restitution. The question is, what should be the antidote? The answer, in part, is technology.

Before the Internet, child pornography consisted of locally produced images—poor quality, expensive, laborious to obtain, hard copy—which were traded among small networks of people.[10] With the advent of the Internet, especially the Dark Web,[11] the distribution of child pornography is now

---

3 18 U.S.C. § 2252A(a)(5)(B), (b)(2) (2012) (Possession of Child Pornography Involving a Prepubescent Minor).

4 Plea Agreement for Def. Mark Wayne Salling, at 12–13, United States v. Salling, No. 2:16-cr-00363-ODW (C.D. Cal. Oct. 3, 2017).

5 *Id.* at 11–12.

6 Salling also possessed a document called "jazzguide," which is "a manual that instructs adult men how to have vaginal and anal intercourse with little girls who are between three and six years old." *Id.* at 13.

7 *Id.* at 12.

8 As this Comment was going through production, Salling committed suicide and was pronounced dead on January 20, 2018. He was reportedly weeks away from sentencing after pleading guilty to possession of child pornography.

9 Salling Plea Agreement, *supra* note 4, at 9, 14; *see also* Joseph Serna, *Former 'Glee' Actor Mark Salling Agrees to Plead Guilty to Possessing Cache of Child Pornography*, L.A. TIMES (Oct. 4, 2017, 1:50 PM), http://www.latimes.com/local/lanow/la-me-ln-mark-salling-plea-20171004-story.html.

10 Amanda Haasz, Note, *Underneath It All: Policing International Child Pornography on the Dark Web*, 43 SYRACUSE J. INT'L L. & COMM. 353, 354–55 (2016).

11 The Dark Web is highly complex but can be defined simply as a portion of the Internet intentionally hidden from search engines, where user's IP addresses are masked, and is accessible only with a special web browser (e.g., "Tor"). Silk Road is probably the most popular example.

an international enterprise.[12] It is thus imperative that law enforcement techniques become commensurate with the threat.

When it comes to combatting child exploitation, strange bedfellows are not so strange after all. Hacktivist group Anonymous and the Federal Bureau of Investigation ("FBI") have something in common: a vehement abhorrence of child pornography.[13] Their weapons of choice, or rather, their methods of detection, share commonalities as well—using technology to fight technology.

The FBI's arsenal ranges from exploiting The Onion Router's ("Tor") anonymous routing system—the system that enables the Dark Web—by setting up honeypots and deploying network investigative techniques ("NITs") that get user-identification data to stick.[14] One of the most recent examples—celebrated by some, maligned by others—is the FBI's Operation Pacifier, the total takedown of the world's largest child pornography website, Playpen.

Salling is but one fish. Playpen is just one pond. Law enforcement should not have to wait in hopes that another Salling will reveal himself. If criminals can become better criminals through technology, law enforcement should become better crime fighters through technology. Specifically, honeypots, NITs, and avatars—Internet crime fighting tools ("ICFT")[15]—are constitutionally permissible and proactive means to combat child exploitation on the Dark Web. But catching the pedophiles is just step one. Step two is identifying, rescuing, and compensating the child victims.

Part I of this Comment provides background: Section A provides an overview of child pornography, the Dark Web, and ICFT; Section B details the FBI's takedown of Playpen (Operation Pacifier). Parts II and III address "concerns." Specifically, using Operation Pacifier as an exemplar, Part II considers Fourth Amendment implications and concludes that ICFT pass constitutional muster. In doing so, Part II offers a potential fix to temper the constitutional concerns. Part III explains that neither an entrapment defense nor an elemental defense is viable. Part IV then transitions to "benefits." In particular, Section A argues how ICFT can provide partial solutions to the dreadful Supreme Court decision *Paroline v. United States*,[16] which made it insurmountably harder for child pornography victims to receive restitution. ICFT will help solve this nonsense by providing tools to identify other pedophile-defendants in the criminal enterprise, enabling victims to receive the restitution they need and are statutorily owed. Section B briefly discusses

---

12 Haasz, *supra* note 10, at 354–55.

13 *See* U.S. DEP'T OF JUSTICE, *Project Safe Childhood Fact Sheet*, https://www.justice.gov/psc/project-safe-childhood-fact-sheet (last updated Apr. 19, 2016); Mark Coppock, *FBI Battling Child Pornographers with Darknet Honeypots and Tor Malware*, DIGITAL TRENDS (Nov. 11, 2016, 10:14 AM), https://www.digitaltrends.com/computing/fbi-running-darknet-child-port-sites-tor-malware/.

14 Coppock, *supra* note 13.

15 For purposes of this Comment, the author coined the terms *NIT*, *honeypots*, and *avatars* collectively as Internet Crime Fighting Tools ("ICFT" for short). This is not a legal or official term.

16 572 U.S. 434 (2014).

findings that a correlation exists between viewers of child pornography and child molesters. Honeypots, NIT, and Sweetie can be effective tools to prevent physical abuse from manifesting. What this Comment does not do is argue for blanket ICFT usage for all crimes.[17] Instead, its focus remains on child pornography, as that crime is particularly heinous, has zero social value, and preys on humanity's most innocent and vulnerable.

I. BACKGROUND

> Children are too important to allow their exploitation by treating criminals like consumers.[18]

The Dark Web has fundamentally altered the topography of crime. The effect technology has had on child pornography is incontestable. What was once intercepted via the mail by Postal Inspectors is now a global game of virtual hide-and-seek—an undertaking involving foreign and domestic law enforcement agencies, cryptocurrency, and technology named after food. Illustrative is the FBI's takedown of Playpen.

A. *Laws and Terms: Child Pornography, the Dark Web, and Honeypots (and Other ICFT)*

Before discussing the constitutional dimensions of ICFT, it is important to provide an overview of the relevant law and to define key terms. It is also critical to demonstrate the criminal nature of child pornography and describe the magnitude of harm it engenders.

1. Child Pornography

"Child pornography" is a bit of a misnomer. "It is important to distinguish child pornography from the more conventional understanding of the term *pornography*."[19] Pornography is generally legal and depicts consenting

---

17 Context matters. NIT should be reserved for the most extreme, heinous crimes. Narcotics and intellectual property infringement, for instance, fall outside that scope. Application in the terrorism context is meritorious. (But that discussion is for another day.) Additionally, the author understands the issue with false witness identification by some child sexual assault victims. Although not as powerful as DNA, using ICFT can potentially serve a similar corroborative (or exonerative) function.

18 Margaret A. Beck, Note, *Emerging Clinical Research Demonstrates the Importance of Adhering to Federal Sentencing Guidelines for Defendants Convicted of Possession of Child Pornography*, 27 U. FLA. J.L. PUB. POL'Y 161, 189 (2016).

19 *Child Pornography*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/criminal-ceos/child-pornography (last updated July 25, 2017) [hereinafter *Child Pornography (DOJ)*].

adults, some of whom are career actors.[20] Child pornography, on the other hand, is child sexual *exploitation*. Each image or video graphically memorializes the sexual abuse of that child. Each child involved in the production of an image or video is a *victim* of sexual abuse—not an actor or willing participant.

Children, by legal definition, cannot consent to their exploitation (*parens patriae*).[21] But child pornography is about more than just legally concocted notions of consent or lack thereof. The act creating the pornography was by force—a rape, for example—and there was unequivocally no consent, legally or commonsensically speaking.

While some child pornography shows children in sheer agony, so the sexual abuse is self-evident, others depict children who appear complacent.[22] A child's complacency, however, is no indication that sexual abuse is absent—oftentimes, a child is threatened or groomed to accept the abuse. In most cases, the abuse is not a singular event, but is instead the product of recurring victimization over months, or even years.[23] Many producers of child pornography cultivate relationships with children in which they gradually sexualize their contact.[24] This "grooming process fosters a false sense of trust," which breaks down the child's resistance to the sexual abuse or desensitizes the child to what is actually happening.[25] In other situations, the criminal is bolder. He threatens to kill the child's parents if she does not follow orders or if she reports him.[26] No young child wants to be a tattletale. Such coercion thus forces abrupt submission and enduringly silences the child. Consequently, even if a child seems complacent, it is imperative to keep in mind that the abuse may have begun years before the video or image was captured.[27] A ticking clock does not make a wrong a right.

The term *child pornography* is used in criminal codes and by lawmakers, prosecutors, law enforcement, and the public to describe recorded child

---

20 For example, Jenna Jameson (1974–). Jameson has been called the world's most famous adult entertainment performer ("The Queen of Porn"). She parlayed that success into an adult media empire. Her company, ClubJenna, was eventually acquired by Playboy and sits in the Fortune 500. She is also a *New York Times* best-selling author. *See Jenna Jameson Biography*, BIOGRAPHY.COM, https://www.biography.com/people/jenna-jameson-381220 (last updated Apr. 2, 2014).

21 *See, e.g.*, Gebardi v. United States, 287 U.S. 112, 118–19 (1932) (holding that the purpose of the Mann Act was to protect females from sexual exploitation and, thus, whether the female willingly or unwillingly crossed state lines for an immoral purpose was irrelevant because the legislature perceived her as a victim; to hold otherwise would frustrate the purpose of the statute if the victim were subject to prosecution as an accomplice in a violation of her own rights).

22 *Child Pornography (DOJ)*, *supra* note 19.

23 *Id.*

24 *Id.*

25 *Id.*

26 *See, e.g.*, Kala Bokelman, *DS Diplomacy Works: Breaking Up a Child Pornography Trafficking Ring*, AM. FOREIGN SERV. ASS'N (June 2018), http://www.afsa.org/ds-diplomacy-works-breaking-child-pornography-trafficking-ring.

27 *Child Pornography (DOJ)*, *supra* note 19.

sexual exploitation.[28] Child pornography, however, fails to describe the true horror suffered by countless innocent child victims.

Some have argued that "merely" possessing child pornography is not that big a deal.[29] Child rape, however, not only carries anatomical consequences,[30] it also alters a child's emotional and psychological wellbeing.[31] And these impacts are even stronger when the abuse is reduced to a recording and put in the criminal marketplace for many more eyes to see.

In a way, possession of child pornography is the economic equivalent of both demand *and* supply. To cut the supply (child exploitation media), you need to cut the demand (possessing the media makes you want more if it), and vice versa. The economic landscape has changed. The costs of producing child pornography are minimal—the price of a new battery on a video camera—but the profits are often enormous.

Statistics and studies demonstrate the Internet's impact on child pornography.

a. *Statistics and Trends: Then and Now*

Even nearly half a century ago, before the omnipresence of the Internet, Congress recognized child pornography as a sordid, ballooning enterprise. "Since the production, distribution[,] and sale of child pornography is often a clandestine operation, it is extremely difficult to determine its full extent. . . . Moreover, because of the vast potential profits involved, it would appear that this sordid enterprise is growing at a rapid rate."[32]

In 1977, Congress concluded "that child pornography and child prostitution have become highly organized, multi*million* dollar industries that operate on a nationwide scale."[33] In that same report, Congress noted that one researcher documented over *260 different magazines* that depicted children—some as young as three—engaged in a range of sexually explicit material, from "lewd poses to intercourse, fellatio, cunnilingus, masturbation, rape, incest[,] and sado-masochism."[34] Congress observed that such pornographic materials were "usually sold either in adult *bookstores or by mail order catalogues*."[35] Most pedophiles preferred the latter because the catalogues were often more customizable, permitting the pedophile to order materials depicting specific sexual deviations.[36] Mail order catalogues also

---

28 *Id.*

29 Beck, *supra* note 18, at 170 (noting John Grisham's statement about his convicted friend).

30 See the horrifying facts of *Kennedy v. Louisiana*, 554 U.S. 407 (2008), discussed *infra* note 96.

31 *See Child Pornography (DOJ)*, *supra* note 19.

32 S. REP. NO. 95-438, at 5 (1977), *reprinted in* 1978 U.S.C.C.A.N. 40, 43.

33 *Id.* (emphasis added).

34 *Id.* at 6 (emphasis added).

35 *Id.* (emphasis added).

36 *Id.*

enabled the pedophile to initiate contact with other pedophiles and to establish liaisons with some of the child "models."[37]

Fast forward to present day. The sordid enterprise worth millions of dollars back in the 1970s is now a multi*billion*-dollar industry.[38] And unsurprisingly, with the advent of the Internet, "260 magazines" pales in comparison to the billions of images now available.[39] Thanks to the 'Net, the network of pedophiles has dwarfed the mail order catalogues of the 1970s.

In 2011, the U.S. Attorney General revealed:

> Unfortunately, we've also 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.[40]

A decrease in age. A disturbing revelation. As to age, one study found that 39 percent of child pornography arrestees possessed images of children aged three to five years, and 19 percent possessed images of infants or toddlers.[41] That means over half of all arrestees analyzed possessed images of children too young or barely old enough to start kindergarten. In 2012, over one-third of juvenile sexual abuse victims were younger than nine years old.[42] As to the level of violence, another study found 80 percent of the arrestees possessed images showing the penetration of a child, and 21 percent possessed images depicting sadistic violence such as bondage, rape, or torture of children.[43]

The growth of the Internet, and especially the Dark Web, has occurred alongside and encouraged the explosion of child pornography as an enterprise.[44] Child pornography is readily available through a cornucopia of Internet-based sources, such as social media sites, file- and photo-sharing sites, gaming devices, and even mobile apps.[45] The Internet does not just act as a museum or marketplace for the predators; it also acts as a source of "community."

---

37 *Id.*

38 STAFF OF H. COMM. ON ENERGY & COMMERCE, 109TH CONG., REP. ON CHILD PORNOGRAPHY 2 (2007).

39 *See id.*

40 *Child Pornography (DOJ)*, *supra* note 19 (quoting then-Attorney General Eric Holder).

41 Janis Wolak et al., *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD. 4 (2005), http://www.unh.edu/ccrc/pdf/jvq/CV81.pdf.

42 U.S. DEP'T OF HEALTH & HUM. SERVS., CHILD.'S BUREAU, *Child Maltreatment 2012* (2012), http://www.acf.hhs.gov/programs/cb/research-data-technology/statistics-research/child-maltreatment.

43 Wolak et al., *supra* note 41, at 5.

44 *Child Pornography (DOJ)*, *supra* note 19.

45 *Id.*

These virtual communities cultivate a collaborative, but corrosive, environment, which thereby promotes more child exploitation. In addition to selling, sharing, and trading child pornography, offenders can connect with each other on Internet forums to share their ideas, interests, desires, and tips, and to brag about their experiences abusing children. Such communication between child pornography offenders fosters a larger relationship premised on a shared sexual interest in children. Masking their true identities, this anonymous community-building erodes the shame that would typically accompany this behavior by bypassing society's ability to scrutinize and condemn it. This groupthink also numbs its members to the victims' physical and psychological damage. Metaphorically, this nurtures an environment where there are many devils on one shoulder and no counterbalancing angel on the other. For these reasons, online communities embolden their members and attract and encourage new peers to join them in the sexual exploitation of children.[46]

An emerging trend is webcam child sex tourism ("WCST").[47] The efforts to combat child sex tourism[48] in impoverished countries led to the unintended consequence of pedophiles seeking the next-best-thing, or perhaps, the perverted latest-and-greatest: puppeteering their own live-streaming sex show. WCST is the convergence of two forms of child sexual exploitation: child pornography and child prostitution. WCST is when adult predators pay to direct and view live-streaming video footage of children in other countries performing sexual acts[49] in front of webcams. These children are often held in "dens."[50] Some WCST victims, however, are not even old enough to communicate or follow the commands.[51] For example, news reports from the Philippines indicate that infants and babies have been rescued.[52] Payment goes to a pimp or madam, who is sometimes the child's own parent.[53] The fee is usually nominal—twenty dollars or so—cheaper than a traditional dinner-and-a-movie.

---

46 *Id.*

47 WCST is also known as "cybersex" in the Philippines and as "live streaming" in some law enforcement reports. Emily Puffer et al., *Webcam Child Sex Tourism: An Emerging Global Issue* (Apr. 16, 2014), https://digitalcommons.cedarville.edu/cgi/viewcontent.cgi?article=1131&context=research_scholarship_symposium.

48 Traditional "child sex tourism" is best described as going on "vacation" in another country to sexually assault children. U.N. HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER, *Combatting Child Sex Tourism*, Apr. 10, 2013, https://www.ohchr.org/en/newsevents/pages/childsextourism.aspx.

49 Child victims of WCST report that they pose naked, masturbate, and have sex with others at the request of these puppeteering predators. SAVE SWEETIE NOW, TERRE DES HOMMES NETHERLANDS, https://www.savesweetienow.org/faq.

50 *Id.*

51 *Id.*

52 *Id.*

53 *Id*.

An estimated tens of thousands of children are victims of WCST in the Philippines alone. A shortage of accurate statistics exists, however, due to WCST's very nature: because it is live, WCST leaves almost no evidence (part of its appeal), and anyway, children rarely report these crimes to police. Notwithstanding, the United Nations and the FBI estimate there are 750,000 predators connected to the Internet at any given moment.[54]

Part of WCST's appeal is that it is less risky. Unlike child sex tourism, WCST does not have the physical risks (travel manifestos) or expenses (flights and hotel) associated with traveling abroad. Further, unlike viewing and downloading traditional child pornography, which is stored on a computer and can be recovered by investigators, live-streaming WCST leaves few, if any, traces of evidence.[55]

Compared to child pornography and child prostitution rings, which are often run by organized criminal syndicates, it is unclear whether WCST has yet been "industrialized" to the same extent. Nevertheless, there has been a rapid increase in the number of largescale WCST operations, often run by non-nationals with links to human trafficking. Without intervention, it is predicted that WCST will rapidly grow into an uncontrollable global industry.[56] Enter Sweetie, which turned these predators into the prey, discussed *infra* Section I.A.3.b.

b. *Snapshot of the Laws*

Child pornography is deservedly among the most heavily punished offenses in criminal law. Child pornography is a crime federally, internationally, and in all fifty states.[57] As discussed *infra* Section I.A.1.c, child pornography is not protected by the First Amendment.[58] Instead, child pornography is illegal contraband under federal law.[59]

---

54 Puffer, *supra* note 47.

55 *See id.*

56 *Id.*

57 However, not all are uniform. State, federal, and international laws differ, sometimes significantly, in their treatment of child pornography offenses. *See, e.g.*, FINDLAW, *State Child Pornography Laws*, http://statelaws.findlaw.com/criminal-laws/child-pornography.html (providing state-specific information, such as definitions and statutes, on all fifty states and the District of Columbia).

58 Federal law distinguishes between (1) pornographic images of an actual minor; and (2) simulated child pornography images, such as those that are not of an actual minor but realistically or intentionally invoke one, and non-realistic images such as "virtual" (computer-generated) images and drawings. The second category is legally protected unless found to be obscene, whereas the first does not require a finding of obscenity. *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 239–40 (2002) (discussed further *infra* Section I.A.1.c).

59 U.S. DEP'T OF JUSTICE, *Citizen's Guide to U.S. Federal Law on Child Pornography*, https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography [hereinafter *Citizen's Guide*].

Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor.[60] "Visual depiction" includes photographs, film, videos, and digital or computer-generated images.[61] Images may be undeveloped and are not required to be stored in a permanent format.[62] Visual depictions also include data stored on a computer disk or by electronic means, which are capable of conversion into visual images.[63]

"Sexually explicit conduct" means "sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person."[64] Thus, the legal definition does not require that an image portray a child engaged in sexual activity with another. A picture of a naked child may constitute child pornography if it is sufficiently sexually suggestive.

Federal law prohibits the production, distribution, importation, reception, and possession of any image of child pornography.[65] "Producing" means "producing, directing, manufacturing, issuing, publishing, or advertising."[66] Inchoate offenses such as attempt and conspiracy also apply in the child pornography context.

The United States Code devotes an entire chapter to child sexual exploitation and abuse: Chapter 110 of Title 18 has twenty-one sections, beginning with § 2251 and ending with § 2260A. Topics include the following: buying or selling children (§ 2251A); the production of child pornography, including its importation into the United States (§§ 2251, 2260); certain activities relating to material involving the sexual exploitation of minors, such as the possession, distribution, and receipt of child pornography (§§ 2252–2252A); misleading domain names, words, or digital images on the Internet (§§ 2252B–2252C); criminal and civil forfeiture (§§ 2253–2254); record keeping requirements (§§ 2257–2257A); definitions (§§ 2256, 2258E); failure to report child abuse (§ 2258); issues involving electronic communication service providers, remote computer service providers, and domain name registrars, such as reporting requirements and limited liability (§§ 2258A–2258B); use to combat child pornography of technical elements relating to images reported to the CyberTipline (§ 2258C); limited liability for the National Center for Missing and Exploited Children (§ 2258D); increased penalties for registered sex offenders (§ 2260A); civil remedy for personal injuries (§ 2255) (proposed legislation); and *mandatory victim restitution* (§ 2259).

---

60 18 U.S.C. § 2256(8) (2012).
61 *Id.* § 2256(5).
62 *Id.*
63 *Id.*
64 *Id.* § 2256(2)(A).
65 *See Id.* §§ 2251, 2252, 2252A.
66 18 U.S.C. § 2256(3).

Victim restitution is currently in flux due to both the Supreme Court's 2014 decision in *Paroline* and Congress's unpassed remedial legislation, which is discussed *infra* Part IV.

Federal jurisdiction attaches if child pornography activity occurs in interstate or foreign commerce.[67] Three points demonstrate the breadth of such attachment: First, if the U.S. Postal Service or another common carrier is used to transport/mail child pornography across state or international borders, federal jurisdiction may attach. Secondly, federal jurisdiction may also attach even if the hard copy image itself did not physically cross a border. For instance, if the materials *used*—such as the computer used to download the images or the blank CD used to store it—originated or traveled at some point in interstate or foreign commerce. Lastly, and most notably, federal jurisdiction almost always attaches when the Internet is used to commit child pornography offenses.[68] Powerfully, an offender can be prosecuted under both state and federal child pornography laws.

Violating child pornography laws is a serious crime for which convicted offenders rightly face not only deep societal condemnation but also statutory punishment, including fines and incarceration.[69] For example, a first-time offender convicted of producing child pornography faces fines and fifteen to thirty years in prison.[70] A first-time offender convicted of transporting child pornography in interstate or foreign commerce faces fines and five to twenty years in prison.[71] Tougher penalties may be levied if the child pornography offense occurred in the following aggravated situations: "(i) the images are violent, sadistic, or masochistic in nature, (ii) the minor was sexually abused, or (iii) the offender has prior convictions for child sexual exploitation."[72] In such circumstances, a convicted offender faces up to life in prison.[73]

---

67 *Citizen's Guide, supra* note 59.

68 *Id.*

69 Curiosity does not always kill the cat. Federal law provides an affirmative defense for those who (1) possess less than three images; or (2) promptly and in good faith took reasonable steps to destroy the image (and did not allow another person to access it) or reported the matter to law enforcement and afforded the agency access to the image. 18 U.S.C. § 1466A(e) (2012).

70 *Id.* § 2251(e).

71 *Id.* § 2252(b)(1).

72 *Citizen's Guide, supra* note 59.

73 *Id.*

c. *Child Pornography Is Not Shielded by the First Amendment—Protecting Children Is a Government Interest of the Highest Order*

> Although I am a [F]irst [A]mendment absolutist, in the area of children I deviate from my absolutism, which is rather strange. It might seem like a contradiction, but bear with me. . . . [I]n the area of children, they must be protected.[74]

Adult pornography is considered a form of personal expression protected by the First Amendment, unless it is obscene (i.e., "patently offensive").[75] Child pornography, however, is not protected.

Over thirty years ago in *New York v. Ferber*,[76] the Supreme Court recognized the evils of child pornography and established that the Constitution does not guard it.[77] The Court ardently declared, "It is evident beyond the need for elaboration that a State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'"[78] The Court highlighted that "[a] democratic society rests, for its continuance, upon the healthy, well-rounded growth of young people into full maturity as citizens."[79] Accordingly, the Court noted, it has "sustained legislation aimed at protecting the physical and emotional well-being of youth even when the laws have operated in the sensitive area of constitutionally protected rights."[80]

The Court asserted that the prevention of child sexual exploitation "constitutes a government objective of surpassing importance."[81] States similarly recognize this grave concern. For example, the legislative findings accompanying passage of the New York laws at issue in *Ferber* reflect this concern:

> [T]here has been a proliferation of exploitation of children as subjects in sexual performances. The care of children is a sacred trust and should not be abused by those who seek to profit

---

74 *Effect of Pornography on Women and Children: Hearings Before the Subcomm. on Juvenile Justice of the Senate Judiciary Comm.*, 98th Cong., 2d Sess. 303–04 (1984) (statement of Al Goldstein, publisher, *Screw*). Mr. Goldstein, a sixteen-year magazine publisher, discussed punishment of sellers and distributors and, by necessary implication, producers of child pornography. He stressed that the abuse of children is appalling and that "anyone who sells photos of child porn should be put away for a long, long time." *Id.* Professor Josephine R. Potuto notes that the quote is "an illustration that the child pornography question makes strange bed-fellows both in terms of the activity depicted and in terms of its troublesome nature for the civil libertarians among us." Josephine R. Potuto, Stanley + Ferber = *The Constitutional Crime of At-Home Child Pornography Possession*, 76 KY. L.J. 15, 15 n.1 (1987).

75 Miller v. California, 413 U.S. 15, 27 (1973).

76 458 U.S. 747 (1982).

77 *Id.* at 757.

78 *Id.* at 756–57 (quoting Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)).

79 *Id.* at 757 (quoting *Prince v. Massachusetts*, 321 U.S. 158, 168 (1944)).

80 *Id.*

81 *Id.*

> through a commercial network based upon the exploitation of children. The public policy of the state demands the protection of children from exploitation through sexual performances.[82]

Ferber, a case now over three decades old, involved videotapes depicting young boys masturbating sold at a bookstore that specialized in sexually oriented products.[83] The explosion of the Internet has drastically changed this landscape, yet *Ferber* recognized the degeneracy of just two videotapes sold at a brick-and-mortar store. The Court's counsel still rings true today and, in a way, served as a warning for things to come. For example, the Court avowed that the distribution of child pornography is intrinsically related to the sexual abuse of children in at least two ways: (1) "the materials produced are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation"; and (2) "the distribution network for child pornography must be closed if the production of material which requires the sexual exploitation of children is to be effectively controlled."[84]

Indeed, the Court understood economics—the supply chain and supply-and-demand. It acknowledged that the "advertising and selling of child pornography provide an economic motive for and are thus an integral part of the production of such materials, an activity illegal throughout the Nation."[85] The Court declared that "there is no serious contention that the legislature was unjustified in believing that it is difficult, if not impossible, to halt the exploitation of children by pursuing only those who produce the photographs and movies."[86] The Court added:

> While the production of pornographic materials is a low-profile, clandestine industry, the need to market the resulting products requires a visible apparatus of distribution. The most expeditious if not the only practical method of law enforcement may be to dry up the market for this material by imposing severe criminal penalties on persons selling, advertising, or otherwise promoting [it].[87]

Later, the Court extended *Ferber* to mere possession of child pornography in *Osborne v. Ohio*.[88]

Child pornography's First Amendment jurisprudence evolved since *Ferber*, and Congress responded with clearer (more strictly worded) statutes. For example, simulated child pornography was made illegal by the Child

---

82 N.Y. LAW, ch. 910, § 1 (1977); *see also* Tex. House Select Committee on Child Pornography: Its Related Causes and Control 32 (1978) ("The act of selling these materials is guaranteeing that there will be additional abuse of children."), *quoted in Ferber*, 458 U.S. at 761 n.13.

83 *Ferber*, 458 U.S. at 752.

84 *Id.* at 759.

85 *Id.* at 761.

86 *Id.* at 759–60.

87 *Id.* at 760.

88 495 U.S. 103 (1990).

Pornography Prevention Act of 1996 ("CPPA"),[89] but the CPPA was short-lived.[90] In *Ashcroft v. Free Speech Coalition*,[91] an adult-entertainment trade association alleged that the CPPA's "appears to be" and "conveys the impression" of-a-minor provisions were vague and overbroad and, thus, restrained works otherwise protected by the First Amendment.[92] The Court agreed. Based on the Court's interpretation of the CPPA, the CPPA banned materials that were neither obscene under *Miller v. California*[93] nor produced by the exploitation of real children as in *Ferber*. Contrasting *Ferber*, Justice Kennedy questionably reasoned that "the CPPA prohibit[ed] speech that record[ed] no crime and create[d] no victims by its production. Virtual child pornography is not 'intrinsically related' to the sexual abuse of children, as were the materials in *Ferber*."[94] The Court further found the CPPA to be inconsistent with *Miller* insofar as the CPPA could not be read to prohibit obscenity because it "lack[ed] the required link between its prohibitions and the affront to community standards."[95] Justice Kennedy held that provisions of the CPPA covered "materials beyond the categories recognized in *Ferber* and *Miller*, and the reasons the Government offers in support of limiting the freedom of speech have no justification in our precedents or in the law of the First Amendment" and abridge "the freedom to engage in a substantial amount of lawful speech."[96] The Court was concerned that the law would

---

89 Pub. L. 104-208, § 121, 110 Stat. 3009 (1996). (At issue were §§ 2256(8)(B), 2256(8)(D) of Title 18, as worded in 2002.)

90 Ashcroft v. Free Speech Coalition, 535 U.S. 234, 244 (2002).

91 535 U.S. 234 (2002).

92 *Id.* at 257.

93 413 U.S. 15 (1973).

94 *Free Speech Coalition*, 535 U.S. at 250 (quoting New York v. Ferber, 458 U.S. 747, 759 (1982)).

95 *Id.* at 249.

96 Justice Kennedy has an interesting history writing for the Court in child exploitation cases—for example, *Paroline v. United States*, 572 U.S. 434 (2014), a case which made it more difficult for victims of child pornography to obtain restitution (as discussed *infra* Part IV), and *Kennedy v. Louisiana*, 554 U.S. 407 (2008), where he held that it is unconstitutional to impose the death penalty for the crime of raping a child, when the victim does not die and death was not intended. The facts of *Kennedy* are revolting. The defendant—who had a history of incest—brutally raped and sodomized his eight-year-old stepdaughter. When police arrived at the home around 9:30 AM, they found the child laying on a bed wrapped in a bloody blanket. She was still bleeding profusely from the vaginal area, despite defendant having previously used a basin of water and a cloth to wipe up the blood, taking any reliable DNA along with it. Police found a trail of blood leading from the garage on the way to the house and up the stairs. The child was rushed to the hospital. A pediatric forensic medicine expert testified that the child's injuries were the most severe he had ever seen. The rape brutally tore the child's perineum from her vaginal opening to her anal opening. It lacerated the interior left wall of her vagina such that it separated her cervix from the back of her vagina, causing her rectum to protrude into her vagina. Immediate, invasive emergency surgery was required to repair these injuries. Defendant concocted a story about how some mystery kids on a blue bicycle raped her in the grass. Police quickly noticed inconsistencies in this tall tale. For one, defendant called his employer three hours early saying he was unavailable for work that day. He called his employer back around 6:30 AM to ask a colleague how to get blood out of a carpet because his daughter had "just become a young lady." At 7:37 AM he called a carpet cleaning service and requested urgent assistance in

make possessors of masterpieces such as William Shakespeare's *Romeo + Juliet* or Academy Award winning movies such as *Traffic* and *American Beauty* subject to severe punishment without inquiry into the work's redeeming, artistic value.[97] The district court had dismissed the overbreadth claim because it was "highly unlikely" that any "adaptations of sexual works like [*Romeo + Juliet*] would be treated as 'criminal contraband.'"[98]

Both Justice O'Connor's concurrence and Chief Justice Rehnquist's dissent expressed concern that rapidly advancing technology would soon make it all but impossible to enforce prohibitions of child pornography.[99] Similarly, both Justices advocated for deference to the legislature and to congressional findings in particular.[100]

Citing *Ferber*, Justice O'Connor emphasized the Court's longstanding recognition that the government has a compelling interest in protecting our nation's children, which is promoted by efforts directed against sex offenders and child pornography.[101] Citing congressional findings, Justice O'Connor noted that the CPPA's ban on virtual child pornography supported these efforts.[102] For example, virtual images "whet the appetites of child molesters,

---

removing bloodstains. The "get-away" bike that defendant identified was found with flat tires, without gears, and was covered in spider webs. Additionally, the grassy area—the fictitious scene of the rape—was undisturbed; instead, blood was found on the underside of the child's mattress in the home. *Kennedy*, 554 U.S. at 413–14. Based on these horrifying facts, a jury of defendant's peers sought to express society's revulsion to such repugnant conduct by sentencing him to capital punishment under Louisiana law. The Louisiana Supreme Court affirmed. But, according to the U.S. Supreme Court, "the death penalty is not a proportional punishment for the rape of a child." *Id.* at 446. The 5–4 opinion, which was joined by the Court's four more liberal-leaning justices, went on to absurdly declare "that there is a distinction between intentional first-degree murder, on the one hand, and non-homicide crimes against individuals, even including child rape, on the other. The latter crimes may be devastating in their harm, as here, but 'in terms of moral depravity and of the injury to the person and to the public, they cannot compare to murder in their severity and irrevocability.'" *Id.* at 410 (quoting Coker v. Georgia, 433 U.S. 584, 598 (1977)). Buttressing the absurdity even more, the Court left open the possibility of the death penalty for "drug kingpin activity" since it is a crime against "the State" rather than against "individual persons." *Id.* at 437. The decision was handed down during the presidential race between Barack Obama and John McCain. Both sharply criticized the majority opinion, on moral grounds and federalism principles. *See* Linda Greenhouse, *Justices Bar Death Penalty for the Rape of a Child*, N.Y. TIMES (June 26, 2008), http://www.nytimes.com/2008/06/26/washington/26scotus.html. Then-candidate Obama opined that "the rape of a small child . . . is a heinous crime, and if a state makes a decision under narrow, limited, well-defined circumstances, that the death penalty is at least potentially applicable, that does not violate our Constitution." McCain passionately called the ruling "an assault on law enforcement's efforts to punish these heinous felons for the most despicable crime. . . . That there is a judge anywhere in America who does not believe that the rape of a child represents the most heinous of crimes, which is deserving of the most serious of punishments, is profoundly disturbing." *Id.*

97 *Free Speech Coalition*, 535 U.S. at 247–48.

98 *Id.* at 243.

99 *Id.* at 264 (O'Connor, J., concurring); *id.* at 267 (Rehnquist, C.J., dissenting).

100 *Id.* at 264 (O'Connor, J., concurring); *id.* at 268 (Rehnquist, C.J., dissenting).

101 *Free Speech Coalition*, 535 U.S. at 263 (O'Connor, J. concurring).

102 *Id.*

who may use the images to seduce young children."[103] Defendants indicted for producing, distributing, or possessing child pornography using real children may evade conviction by claiming that the images are technically computer-generated.[104]

Congress and President George W. Bush responded to *Free Speech Coalition* by enacting the PROTECT Act of 2003 (also known as the "Amber Alert law").[105] Patching up the CPPA's unconstitutional language, the law criminalized visual depictions

> of any kind, including a drawing, cartoon, sculpture, or painting—that depicts a minor engaging in sexually explicit conduct; *and is obscene*; or depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse *. . . and lacks serious literary, artistic, political, or scientific value*."[106]

The statute further made clear that the minor depicted did not need to actually exist.[107]

This new wording was tested and upheld in 2008 in *United States v. Whorley*.[108] The defendant, who was already on probation for a 1999 federal child pornography conviction, was convicted under 18 U.S.C. § 1466A for using a public computer to receive and print obscene Japanese anime cartoons that graphically depicted adult males sadistically and violently raping prepubescent girls.[109] He also possessed child pornography involving real children and twenty sexually explicit emails describing child incest and molestation by physicians.[110] Whorley challenged the statute, arguing it violated the First Amendment.[111] The Fourth Circuit found the statute unambiguous because it explicitly states that it is not a required element that the minor depicted actually exist, and "[t]he clear language of [the statute] is sufficiently broad to prohibit receipt of obscene cartoons . . . ."[112]

---

103 *Id.* (citations omitted).

104 *Id.* Acknowledging that respondents may be correct that, at the time, no defendant successfully employed this tactic, Justice O'Connor stressed that "given the rapid pace of advances in computer-graphics technology, the Government's concern [was] reasonable. Computer-generated images lodged with the Court by *amici curiae* . . . [bore] a remarkable likeness to actual human beings." *Id.* at 264. She opined that "[a]nyone who has seen, for example, the film *Final Fantasy: The Spirits Within* (H. Sakaguchi and M. Sakakibara directors, 2001) can understand the Government's concern." *Id.* Furthermore, Justice O'Connor pointed out that the "Court's cases do not require Congress to wait for harm to occur before it can legislate against it." *Free Speech Coalition*, 535 U.S. at 263 (O'Connor, J. concurring) (citing Turner Broadcasting System, Inc. v. FCC, 520 U.S. 180, 212 (1997)).

105 18 U.S.C. § 1466A (2012).

106 *Id.* § 1466A(a) (emphases added).

107 *Id.* § 1466A(c).

108 550 F.3d 326 (4th Cir. 2008), *cert. denied*, 558 U.S. 1117 (2010).

109 *Id.* at 331.

110 *Id.*

111 *Id.* at 332.

112 *Id.* at 336 (first alteration in original).

The PROTECT Act also amended 18 U.S.C. § 2252A by adding paragraph (a)(3), which criminalizes knowingly advertising or distributing "an obscene visual depiction of a minor engaging in sexually explicit conduct; or a visual depiction of an actual minor engaging in sexually explicit conduct."[113] The law draws a distinction between the obscene depiction of *any* minor and the mere depiction of an *actual* minor. By adding the word "obscene," the amendments to "virtual" or computer-generated images (which were originally deemed unconstitutional under *Free Speech Coalition*) passed the *Miller* test.

Also in 2008, the Supreme Court in *United States v. Williams*[114] upheld the 2003 amendment to § 2252A(a)(3)(B), which criminalizes the pandering and solicitation of child pornography.[115] In a 7–2 decision penned by the late Justice Scalia, the Court reversed the Eleventh Circuit's holding that the law was unconstitutionally vague.[116] To hold otherwise would deeply hamper law enforcement's ability to fight child pornography. As the Court explained, instead of targeting the underlying material (child pornography), the statute bans the collateral speech (solicitation) that introduces such material into the child-pornography distribution network.[117] "Thus, an Internet user who solicits child pornography from an undercover agent violates the statute, even if the officer possesses no child pornography."[118]

In sum, child pornography is illegal in the United States and is not viewed through the normal First Amendment lens. This is because child pornography always harms the child when it is made, sold, shared, and possessed, and the government's interest in preventing such is of the highest order.

d. *Psychological Impact of Reproduction on the Internet*

Child pornography is a vicious circle from which children almost never escape. It starts with the sexual abuse, moves to its recordation, and continues with its dissemination on the Internet, all which result in the perpetual revictimization of the child. The circumference of this child pornography circle psychologically traps the child inside.

In other words, child pornography creates a permanent record of a child's sexual abuse. As such, it exponentially exacerbates the threat and harm to a child victim more than does the sexual abuse itself.[119] The child's

---

113 18 U.S.C. § 2252A(a)(3)(B) (2012).

114 553 U.S. 285 (2008).

115 *Id.* at 307.

116 *Id.* at 287, 307.

117 *Id.* at 293.

118 *Id.*

119 *See, e.g.*, T. Christopher Donnelly, *Protection of Children from Use in Pornography: Toward Constitutional and Enforceable Legislation*, 12 U. MICH. J.L. REFORM 295, 301 (1979) (interview with a

awareness that his or her abuse is reduced to a recording and circulated for perverted audiences worldwide may haunt the child long after the original crime took place.[120] A child who has posed for the pedophile's camera or starred in his sick show must go through life knowing that that photo or that video is circulating within child pornography's mass distribution system.[121] "[I]t is the fear of exposure and the tension of keeping the act secret that seem to have the most profound emotional repercussions."[122] Like a Tetris of trauma.

Because the revictimization continues in perpetuity, it leads to lasting psychological damage, such as debilitating anxiety and depression; feelings of helplessness, humiliation, and fear; self-image issues such as a lack of self-worth; separation anxiety; aggression; nightmares; disruptions in sexual development; problems building trusting relationships; and suicide.[123]

The distribution of child pornography can also lead to further revictimization not just in the emotional or psychological senses, but in the physical molestation sense, too. Viewers of child pornography may demand more videos of a particular child if they like what they see. Likewise, the producer may ramp up his production—by either increasing the exploitation of his original victim or by finding a new victim—because a particular video has garnered him "fame" and "fortune."

Once an image is on the Internet, it is downloadable by the masses, thus making it irrevocable. Sadly, emerging trends reveal an increase in the number of images depicting sadistic and violent child sexual abuse with a corresponding decrease in victim age. For example, the number of images depicting very young children, including toddlers and infants, has increased.[124] Undoubtedly, this will increase the physical and psychological instability of child pornography victims.

2. The Onion Router and Its Evolution to the Dark Side: The Dark Web

Tor was the brainchild of the U.S. Naval Research Laboratory, devised to protect sensitive government communications.[125] Now, Tor is publicly accessible, and it has undergone a metamorphosis. Tor and its cousin networks

---

child psychiatrist) ("The victim's knowledge of publication of the visual material increases the emotional and psychic harm suffered by the child.").

120 *See, e.g.*, David P. Shouvlin, *Preventing the Sexual Exploitation of Children: A Model Act*, 17 WAKE FOREST L. REV. 535, 545 (1981).

121 *Id.*

122 Ulrich C. Schoettle, *Child Exploitation: A Study of Child Pornography*, 19 J. AM. ACAD. CHILD PSYCHIATRY 289, 292 (1980).

123 *See, e.g.*, *id.* at 295.

124 *Child Pornography (DOJ)*, *supra* note 19.

125 United States v. Matish, 193 F. Supp. 3d 585, 593 (E.D. Va. 2016).

collectively make up the Dark Web family. Tor was born to anonymize Internet usage. Specifically, Tor provides anonymity to Internet users "by masking their user data and hiding information by funneling it through a series of interconnected computers."[126] Over 1000 servers exist in the Tor network worldwide.[127] "Because Tor attempts to keep users' IP addresses hidden, the Government cannot rely on traditional identification techniques to identify website visitors who utilize the Tor network"[128] to carry out their crimes.[129]

This Onion has two halves. The first is downloadable software. The second is a volunteer network of computers creating "hidden services." Tor allows hidden services to operate only within the Tor network. Anyone can download the Tor browser from the Tor website. Then, users can search indexed websites of Tor hidden services; these indexes behave differently than typical search engines like Bing or Google.[130] "[P]eople who log into a hidden service cannot identify or locate the website itself."[131] Similarly, Tor enables its users to access the Internet anonymously.[132] With the "regular" Internet, a website's operator can usually identify visitors to the site through the visitors' IP addresses. Tor, on the other hand, keeps users' IP addresses hidden.[133] It does so by routing web traffic across several different "relays" or servers, and then encrypting that traffic. These maneuvers result in the appearance that the user's IP address is coming from the IP address of a Tor exit relay. Communications on hidden services are also encrypted. Tor provides mirror image services: it offers obscurity both to a hidden service's operator and to its visitors. Thus, Tor is an armor of anonymity, alluring those seeking to engage in nefarious activities.[134]

A preliminary caveat is in order. The Dark Web is not all bad. In fact, there is a good side, as many people and organizations use Tor for legal and legitimate purposes.[135] For example, Tor is used as a free speech platform because it supplies safe fora for whistleblowers, journalists, and the politically oppressed.[136]

---

126 U.S. Dep't of Homeland Security, *Case Summaries: Circuit Courts of Appeal*, FEDERAL LAW ENFORCEMENT INFORMER, Nov. 2017, at 11, 12 [hereinafter INFORMER].

127 *Matish*, 193 F. Supp. 3d at 594.

128 *Id.*

129 To shield their enterprise from law enforcement eyes, several online criminal organizations have written security manuals instructing their members to follow strict security protocols and encryption techniques. *See Child Pornography (DOJ)*, *supra* note 19.

130 *Matish*, 193 F. Supp. 3d at 594.

131 *Id.*

132 *Id.* at 593.

133 *Id.* at 594.

134 "The wicked flee when no man pursueth" (Proverbs 28:1), *quoted in* California v. Hodari D., 499 U.S. 621, 623 n.1 (1991)).

135 *Matish*, 193 F. Supp. 3d at 585, 593.

136 *See, e.g.*, United States v. Focia, 869 F.3d 1269, 1274 n.1 (11th Cir. 2017).

But characteristically, the Dark Web is "dark"; it conjures up an underworld where virtually anything can be bought and sold if the price is right.[137] It is not your everyday local farmer's market. This cauldron is a borderless marketplace chockful of illegal firearms,[138] narcotics,[139] stolen and fraudulent identification documents,[140] toxic chemicals,[141] murder-for-hire, and humans. It is also the main source of child pornography. Users essentially transact with ghosts. And these transactions leave almost no cookie crumbs.[142]

Over 1000 servers all over the world exist in the Tor network.[143] "Because Tor attempts to keep users' IP addresses hidden, the Government cannot rely on traditional identification techniques to identify website visitors who utilize the Tor network."[144] The methods many child pornography offenders use to dodge detection have greatly changed since the days when Postal Inspectors would intercept the illicit mail. Now, the methods have become increasingly sophisticated, sometimes state-of-the-art, and predators are better at evading law enforcement. Purveyors of child pornography use encryption techniques and anonymous networks on the Dark Web to hide their amassed inventory of illegal child abuse images.

3. Honeypots, NITs, and Sweetie: Internet Crime Fighting Tools

Honeypots, NIT, and Sweetie make up the hornet's nest for fighting child pornography on the Dark Web.

a. *Honeypots and NITs*

As its name suggests, a honeypot is designed to attract and stick. "A honeypot or deception host is a designated area within a computer system or

---

137 *See, e.g.*, *id.* at 1274.

138 *Id.* (remarking that the defendants used a website called Black Market Reloaded to sell firearms).

139 U.S. DEP'T OF JUSTICE, *ALPHABAY, THE LARGEST ONLINE 'DARK MARKET,' SHUT DOWN*, Press Release 17-803 (July 20, 2017), https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

140 *Id.*

141 *Id.*

142 Cryptocurrency is the medium of exchange on the Dark Web. Like the Dark Web, its defining feature is its anonymous nature, making it well-suited for money laundering and buying contraband. Cryptocurrency, like Bitcoin and its derivatives, uses decentralized control as opposed to centralized banking systems such as the Federal Reserve System. This is accomplished through an encrypted blockchain, which is essentially a digital, decentralized ledger. Because the virtual currency is not issued by a central authority (such as a government), it is theoretically immune to government interference. *See Cryptocurrency*, INVESTOPEDIA, https://www.investopedia.com/terms/c/cryptocurrency.asp (last visited Dec. 14, 2017).

143 *Matish*, 193 F. Supp. 3d at 594.

144 *Id.*

network that has been designed specifically with the expectation that it will be attacked by unauthorized users, whether internal or external to the organization operating the honeypot."[145] Honeypots are not just used to catch potential hackers.

In the child pornography realm, "[h]oneypot traps are sites that purport to contain child pornography but in fact are set up by police and are designed to capture the IP address or credit card details of visitors trying to download images."[146] Honeypots are essentially passive decoys or copies of target websites. Honeypots provide law enforcement with the ability to capture "detailed and contemporaneous forensic evidence"[147] about the bees that took the bait.

Once a target is "attracted" to the honeypot, NIT is deployed. NIT is essentially code that bypasses Tor protections to grab a user's IP address and other potential identifiers.[148] Privacy advocates see it a different way, calling it disseminating "malicious software" (malware).[149] It is no such thing.

b. *Sweetie*

Another promising ICFT is Sweetie. Sweetie is an Internet avatar—a computer-animated, photorealistic image of a ten-year-old Filipina girl.[150] In 2013, the Dutch branch of the children's rights organization Terr des Hommes and a local animation company gave birth to Sweetie in an effort to combat the growing problem of WCST.[151]

Sweetie had the following modus operandi: the virtual girl would enter a chat room.[152] Within seconds, like sharks, predatory men would circle. Once approached, "Sweetie" would write that she was a ten-year-old girl from the Philippines.[153] Undeterred, the sexual predators would then open a webcam connection with Sweetie, at which point programmers would animate her in real time through motion capture as the situation unfolded.[154]

---

145 Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape?*, 29 RUTGERS COMPUTER & TECH. L.J. 317, 318 (2003).

146 Richard Wortley & Stephen Smallbone, INTERNET CHILD PORNOGRAPHY: CAUSES, INVESTIGATION, AND PREVENTION 60 (Graeme R. Newman ed. 2012).

147 Walden & Flanagan, *supra* note 145, at 317.

148 NIT is discussed in greater detail *infra* Section I.B.

149 *See* Coppock, *supra* note 13.

150 SAVE SWEETIE NOW!, TERRE DES HOMMES NETHERLANDS, https://www.savesweetienow.org. An informative video summarizing Sweetie can be found at https://www.youtube.com/watch?v=y WLTEkryAQg.

151 *Id.*

152 *Id.*

153 *Id.*

154 *Id.*

During the ten-week research period, predators requested the "child" perform a broad range of sexual acts including smoking cigarettes while naked, masturbating, eating feces, having sex with older men, and having sex with family members.[155] As the dialogue between Sweetie and the predator progressed, the predator would make a wire transfer and provide his Skype address. At that point, the chat would shut down and the identifying information would be recorded.[156] The data was then given to EUROPOL/Interpol.[157]

Within ten weeks, this technology identified over 1000 predators in seventy-one countries.[158] Resulting arrests and convictions took place in countries such as Australia, Belgium, Denmark, the Netherlands, Poland, and the United Kingdom.[159] Importantly, child victims were also identified and rescued from the cybersex dens.[160]

Many American predators were recorded from the webcam; researchers could actually see their faces and their family pictures in the background.[161] Sweetie's director, Albert Jaap Van Santbrink, said, "That's the scariest part. They are fathers, husbands, partners, ordinary people you meet every day."[162]

Sweetie is not without controversy. Opponents contend that Sweetie served as an illegal sting operation; and because it may have entrapped predators, any data sourced from Sweetie is inadmissible.[163] However unorthodox though, this cutting-edge approach is opening new opportunities for cooperation among international agencies to prevent these twenty-first century cybercrimes against children.[164]

Partly in response to Sweetie's critics, Sweetie is getting a sister. Sweetie 2.0 is being developed in concert with programmers, legal and law enforcement specialists, forensic psychologists, and cybercrime experts.[165] Sweetie 2.0 will act as an "early warning system" aimed at alerting potential child abusers to the illegality of their proposed activities.[166] It will

---

155 SAVE SWEETIE NOW, TERRE DES HOMMES NETHERLANDS, https://www.savesweetienow.org/faq (last visited Nov. 18, 2018).

156 SAVE SWEETIE NOW, TERRE DES HOMMES NETHERLANDS, https://www.savesweetienow.org/about-us (last visited Nov. 18, 2018) [hereinafter *Save Sweetie: About Us*].

157 *Id.*

158 *Id.*

159 *Id.*

160 *Id.*

161 Dragana Jovanovic, *'Sweetie' Sting Lures Thousands of Alleged Pedophiles*, ABC NEWS (Nov. 5, 2013), http://abcnews.go.com/International/sweetie-sting-lures-thousands-alleged-pedophiles/story?id=20792348.

162 *Id.*

163 Kristen Schweizer, *Avatar Sweetie Exposes Sex Predators*, THE AGE (Apr. 26, 2014, 3:00 AM), https://www.theage.com.au/world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html.

164 *Save Sweetie: About Us*, *supra* note 156.

165 SAVE SWEETIE NOW, TERRE DES HOMMES NETHERLANDS, https://www.savesweetienow.org/how-we-work (last visited Nov. 18, 2018).

166 *Id.*

recommend that the individuals seek help and will provide links to referral agencies.[167] More than just a "gotcha" device, Sweetie 2.0 seeks to "pioneer and monitor this approach as a deterrent" for what forensic psychologists call "curious cats."[168] As discussed *supra* Section I.A.1.a, many perpetrators of child sexual abuse justify their aberrations "by joining online peer groups with similar interests and persuasive tendencies."[169] Stark reminders about the criminality and devastating effects of child sexual abuse could stop some people from proceeding.[170]

The initial Sweetie deployment satisfied its dual intention of both drawing attention to the online sexual exploitation of children and demonstrating that identifying potential child abusers and victims is relatively simple. Sweetie turned its predators into prey.

Classic reactive law enforcement policies mean law enforcement cannot investigate child exploitation until crimes are reported. But child victims usually do not report the crimes. So Sweetie encourages proactive investigative techniques.[171] Furthermore, Sweetie does not implicate the Fourth Amendment because there is no search, and as discussed *infra* Part III, it is also not an entrapment device.

B. *Operation Pacifier: Laudable or Lamentable?*

As its name disturbingly suggests, Playpen was a wretched platform for the sexual exploitation of children. Dubbed the "largest remaining known child pornography [website] in the world," Playpen thrived because of its status on the Dark Web[172]—that is, until Operation Pacifier.

The operation was unprecedented in its scope and reach. It opened up new avenues for international cooperation in efforts to prosecute child abusers around the world. But the "how" has caused mixed reactions. To many, including the author of this Comment, Operation Pacifier was ingenious and a true success story. To others, it was an egregious violation of the Constitution. As demonstrated *infra* Parts II and III, it was no such thing; indeed, Part IV explains why similar operations should be encouraged.

---

167 *Id.*

168 *Id.*

169 *Id.*

170 *Id.*

171 *See* SAVE SWEETIE NOW, *supra* note 165.

172 Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, MOTHERBOARD (Jan. 5, 2016, 4:00 PM), https://motherboard.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

1. Playpen

Just a month after its launch in the summer of 2014, Playpen had nearly 60,000 registered member accounts.[173] This number ballooned to over 200,000 registered users by early 2015.[174] Still in its nascent stage, Playpen had an average of 11,000 unique visitors each week and 117,000 total posts.[175] According to FBI testimony, many of these posts contained extreme depictions of child abuse, the worst anyone could imagine.[176]

Playpen was both a catalogue and a forum. Members uploaded and viewed tens of thousands of licentious postings of children, indexed by age, gender, and sexual activity.[177] Playpen contained a forum for discussing all things pedophilic, including tips on grooming child victims and eluding detection.[178] Playpen's victims were both domestic and foreign, some of whom the Government knew.[179]

Playpen's creator was a fifty-eight-year-old Florida man, Steven W. Chase.[180] Unbeknownst to Chase, his secret site had a slip up. Playpen's IP address was exposed due to a misconfiguration in Firefox, a critical blunder.[181]

2. Operation Pacifier: The Bulldozing of Playpen

In December 2014, a foreign law enforcement agency notified the FBI of its suspicion that Playpen's IP address was U.S.-based.[182] From that point on, the FBI took typical investigative steps: it served search warrants for email accounts and followed the money.[183] This led the FBI to Chase and his two cohorts, Playpen administrators Michael Fluckiger, forty-six, of Indiana, and David Browning, forty-seven, of Kentucky.[184] All three were arrested and sentenced to lengthy prison terms—thirty years for Chase and twenty years

---

173 *Id.*

174 *Id.*; *see also* United States v. Matish, 193 F. Supp. 3d 585, 594 (E.D. Va. 2016). Of note, before signing up for an account, potential registrants were warned to use a fake email address and avoid identifying information on their profiles. *Id.*

175 Cox, *supra* note 172; *Matish*, 193 F. Supp. 3d at 594.

176 Cox, *supra* note 172; *Matish*, 193 F. Supp. 3d at 594.

177 *'Playpen' Creator Sentenced to 30 Years*, FBI.GOV (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

178 *Matish*, 193 F. Supp. 3d at 594.

179 *Id.*

180 *'Playpen' Creator Sentenced to 30 Years*, *supra* note 177.

181 Cox, *supra* note 172.

182 United States v. Darby, 190 F. Supp. 3d 520, 526 (E.D. Va. 2016).

183 *'Playpen' Creator Sentenced to 30 Years*, *supra* note 177.

184 *Id.*

each for Fluckiger and Browning.[185] Although the FBI cut the head of the snake, there was more work to be done.

The FBI, in partnership with the Department of Justice's Child Exploitation and Obscenity Section, launched Operation Pacifier—an effort to bring Playpen's thousands of members to justice.[186] Using the court-approved and innovative NIT, agents began identifying Playpen users.[187]

In January 2015, armed with a search warrant, the FBI seized the host server in North Carolina and relocated the website's content to servers in a secure government facility in the Eastern District of Virginia.[188]

Rather than completely shutting down the site—and missing the golden opportunity to identify those who produced, distributed, or possessed child pornography—the FBI assumed administrative control over Playpen for a limited time.[189] The FBI turned Playpen into a honeypot. But although it could monitor Playpen traffic, Tor's encryption technology prevented the FBI from determining who the drivers were.[190] So, to unveil Playpen visitors' IP addresses, in February 2015, the FBI sought a warrant from a federal magistrate judge in the Eastern District of Virginia that would allow it to deploy a state-of-the-art NIT.[191]

The mechanics of Operation Pacifier's NIT deployment are pertinent. As described in the warrant affidavit, "when an individual visits a website the website sends 'content' to the individual. This content is downloaded by the individual's computer and used to display the webpage on the computer."[192] Deploying a NIT "augments the content with additional instructions."[193] The NIT deployed in Playpen instructed any "activating computer"—a computer that logged into Playpen by entering a username and password—to send certain information to a computer "controlled by or known to the government."[194] The NIT transmitted the following information, with timestamps, from the activating computer: (1) the IP address; (2) a unique identifier generated by the NIT to distinguish the activating computer's data from that of others; (3) the operating system and architecture (e.g., Windows 7); (4) the operating system username; (5) information about whether the NIT was already sent to the computer; (6) the host name; and (7)

---

185 *Id*.

186 *Id.*

187 *Id.*

188 *Id.*; INFORMER, *supra* note 126, at 12.

189 *Darby*, 190 F. Supp. 3d at 526.

190 *See id.* Normally a website administrator can readily identify the IP addresses of the site's visitors. However, on Tor, the administrator can identify the IP address of only the exit node, which is not the same as the visitor's IP address. *Id.* at 526.

191 *Id.*

192 *Id.* (citation omitted).

193 *Id.*

194 *Darby*, 190 F. Supp. 3d at 526.

the media access control ("MAC") address.[195] Notably, it was limited to computers "of any user or administrator who log[ged] into [Playpen] by entering a username and password."[196]

The warrant—whose affiant was a nineteen-year law enforcement veteran—was granted.[197] The warrant permitted the FBI to run Playpen from a location in the Eastern District of Virginia and deploy the NIT for thirty days.[198] Once the NIT was activated, the FBI sent subpoenas to Internet Service Providers ("ISPs") like Verizon and Time Warner.[199] The ISPs provided the names, subscriber information, and addresses.[200] Armed with this information, the FBI obtained individual warrants to search the homes of the identified Playpen users.[201] Unsurprisingly, the FBI found child pornography on these users' home computers.[202]

Operation Pacifier was a tremendous success. In addition to taking down the website, the ongoing investigation has produced the following results (as of May 4, 2017):

* At least 350 U.S.-based individuals arrested.
* 25 producers of child pornography prosecuted.
* 51 hands-on abusers prosecuted.
* 55 American children successfully identified or rescued.
* 548 international arrests, with 296 sexually abused children identified or rescued.[203]

Despite this victory, not all were amused. A swarm of defendants moved to suppress. Defendants alleged, in part, that the NIT warrant was unsupported by probable cause and that it was issued by a magistrate without jurisdictional authority.[204] Well-funded digital rights groups lamented that the sky was falling.[205]

---

195 *Id.* at 526–27; United States v. Matish, 193 F. Supp. 3d 585, 595 (E.D. Va. 2016).

196 *Matish*, 193 F. Supp. 3d at 594–95 (second alteration in original).

197 *Id.* at 595.

198 *Darby*, 190 F. Supp. 3d at 527.

199 *Id.*

200 *Id.*

201 In one case alone, the defendant possessed 1608 images and 298 videos of child pornography. *Id.* Another had over 20,000 files on his personal computers. United States v. Tagg, 866 F.3d 579, 585 (6th Cir. 2018).

202 *Darby*, 190 F. Supp. 3d at 527.

203 *'Playpen' Creator Sentenced to 30 Years*, *supra* note 177.

204 *Darby*, 190 F. Supp. 3d at 530.

205 *See, e.g.*, Mark Rumold, *Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation*, ELECTRONIC FRONTIER FOUND. (Sept. 15, 2016), https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation (describing such groups' views).

Defendants and privacy advocates bemoaned that the Playpen operation was "illegal."[206] Using borderline Chicken Little reasoning, they believed the operation entrapped users and that the NIT amounted to dragnet government "hacking" in violation of users' Fourth Amendment rights.[207] They opined that the courts' upholding of the FBI's actions were "dangerous decisions" that threatened to undermine constitutional privacy protections in personal computers "for all of us."[208]

Despite these unamused parties, Operation Pacifier was held (and continues to be held) constitutional by many federal district and circuit courts.[209] The FBI used technology to fight technology, and by doing so, it saved hundreds if not thousands of children from further exploitation.[210]

Although it has been four years since Playpen's extermination, similar sites continue to pop up and proliferate on the Dark Web. As Special Agent Dan Alfin of the FBI's Violent Crimes Against Children Section put it:

> It's ongoing and we continue to address the threat to the best of our abilities. It's the same with any criminal violation: As they get smarter, we adapt, we find them. It's a cat-and-mouse game, except it's not a game. Kids are being abused, and it's our job to stop that.[211]

Nowhere on this planet is immune from people who seek to sexually exploit children through child pornography. Technology has created a child pornography chain: it enables the continuous production and distribution of child pornography, which increases the demand for new and more egregious images, thereby perpetuating the continued molestation of child victims as well as the abuse of new children. Technology has also erected a barbed wire fence around this chain, by using encryption and the Dark Web to insulate child predators from law enforcement. Accordingly, law enforcement must use technology as a weapon to abate technology as a fortress.

II. HONEYPOTS (AND OTHER ICFT) FIT SQUARELY WITHIN THE CONFINES OF THE FOURTH AMENDMENT

In tackling the scourge of child pornography, law enforcement and legislators are finding that it is not unlike some difficult marriages—all but impossible to fix, but also impossible to end. Child pornography is like a cancer, metastasizing and replicating at astonishing rates due to technology. As such,

---

206 *Id.*

207 *Id.*

208 *Id.*

209 Indeed, contrary to privacy advocates' fears, there is recourse for willful violations—an aggrieved party can seek damages under 18 U.S.C. § 2712 (Patriot Act–based violations).

210 *'Playpen' Creator Sentenced to 30 Years*, *supra* note 177.

211 *Id.*

law enforcement must be permitted to use technology, such as honeypots and NITs, as surgical tools to quell child pornography's cancerous ways.

Privacy is sacred to every American. The Government must not gain a perpetual license to arbitrarily rummage around law-abiding citizens' computers and read emails. However, it is axiomatic that possessors of child pornography are not law-abiding citizens. It is further obvious that the Fourth Amendment protects only against *unreasonable* searches.

Deploying a NIT is not a Fourth Amendment search. Using ICFT is not a search for the following reasons: one does not have a reasonable expectation of privacy in contraband, which child pornography is; and the third-party and assumption of risk doctrines apply to ICFT.

Specifically addressing the Playpen NIT, even if courts deem it a search, it was certainly a reasonable one. Moreover, the FBI was armed with a warrant. Even if the warrant was defective, the NIT "search" does not require exclusion per the *Leon*[212] good faith exception.

A. *Warrantless "Searches" of Internet Identifiers Are Constitutionally Permissible Because of the Third-Party and Assumption of Risk Doctrines*

If we assume NIT is a "search" under the Fourth Amendment, we can easily argue that the search is reasonable. This is true whether viewed through the reasonable-expectation-of-privacy lens of *Katz*[213] or the traditional trespassory approach of *Jones*.[214]

1. No Reasonable Expectation of Privacy in Contraband

child pornography is contraband. There is no legal use for it.

2. No Reasonable Expectation of Privacy in Your IP Address or What You Willingly Expose to the Public

"[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[215] In developing the third-party doctrine, the Supreme Court in *Smith v. Maryland*[216] held that there is no reasonable expectation of privacy in phone numbers dialed.[217] Since then, the Court has generally held that the government may obtain information without a warrant when an individual makes similar data available to a third party.[218]

---

212 United States v. Leon, 468 U.S. 897 (1984).

213 Katz v. United States, 389 U.S. 347 (1967).

214 United States v. Jones, 565 U.S. 400 (2012).

215 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

216 442 U.S. 735 (1979).

217 *Id.* at 743–44

218 *See, e.g.*, *Smith*, 442 U.S. at 743–44; United States v. Miller, 425 U.S. 435, 442 (1976) (no reasonable expectation of privacy in information voluntarily conveyed to the bank). As technology has

Using the NIT to capture IP addresses is akin to using pen registers to see numbers dialed, which the Court found constitutional even when Federal Rule of Criminal Procedure 41 ("Rule 41") did not specifically include electronic intrusions in its definition of property.[219] Like the pen registers in *Smith*, IP addresses do not capture the *content* of communications; once the NIT identifies an IP address, it does not then observe *all* Internet traffic or read private emails.

Under the *Katz* dual-pronged reasonable-expectation-of-privacy test, one does not have a reasonable expectation of privacy in his IP address, even on the Dark Web. Although it may be subjectively reasonable, it is not objectively reasonable. Masking your identity via Tor is akin to simply putting on a ski mask as you rob a bank outfitted with security cameras. There is no constitutional reward for being a sly fox.

Indeed, in the Playpen cases, courts have ruled that a defendant's subjective expectation that his IP address would remain private through his use of Tor so that he could obtain child pornography is not one any humane society is prepared to recognize as reasonable.[220] Defendants cannot "serendipitously receive Fourth Amendment protection" because they used Tor to evade detection, while individuals who do not hide their IP addresses are not protected by the same constitutional safeguards.[221] Accordingly, the FBI's use of the NIT, *even though executed pursuant to a search warrant*, could not be considered a search under the Fourth Amendment, and any purported violation of the magistrate's venue authority was not a constitutional one.[222]

The notion of "false friends" further demonstrates a lack of legitimate expectations of privacy. The Supreme Court has repeatedly affirmed the use of undercover agents to conduct conversational surveillance, holding that such activity does not implicate the Fourth Amendment.[223] The Court has

---

evolved and as smartphones have become ubiquitous, however, the third-party doctrine has become controversial, if not weakened. For example, the Supreme Court decided (right before this Comment's publication) *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The Court considered whether the warrantless seizure and search of historical cellsite records revealing the location and movements of a cellphone user over the course of 127 days was permitted by the Fourth Amendment. The Court, in a 5–4 decision by Chief Justice Roberts (with an excellent dissent by Justice Gorsuch), answered no. The holding, fortunately, appears to be a narrow one. Tying the holding to this Comment and the FBI's NIT, the NIT was temporally limited to thirty days, almost three-quarters less than the time in *Carpenter*.

219 United States v. N.Y. Tele. Co., 434 U.S. 159, 169–70 (1977).

220 United States v. Matish, 193 F. Supp. 3d 585, 616 (E.D. Va. 2016); United States v. Werdene, 188 F. Supp. 3d 431, 446 (E.D. Pa. 2016).

221 *Werdene*, 188 F. Supp. 3d at 446 (quoting United States v. Stanley, 753 F.3d 114, 121 (3d Cir. 2014)).

222 *Id.*

223 *See* United States v. White, 401 U.S. 745 (1971) (holding that conversations recorded and monitored at various locations, including defendant's home, by use of a concealed radio transmitter worn by an informant was not an unreasonable search/seizure and thus did not require a warrant); Hoffa v. United States, 385 U.S. 293 (1966) ("[I]t is evident that no interest legitimately protected by the Fourth

tolerated this investigative technique, likely because it "pragmatic[ally] recogni[zes]" that "false friends" is an essential way to detect otherwise inaccessible information about crime.[224] Such recognition occurred nearly fifty years ago in *Hoffa v. United States*[225] and *United States v. White*;[226] it is even truer now with the "going Dark" dilemma.

NIT is like a "wired friend" but is even less invasive because it does not record purportedly private conversations. Playpen users assumed the risk that their "friends" might be foes when they logged into the Dark Web hidden service and posted on forums.

Quite simply, the Dark Web does not confer a user the right to "be let alone."[227]

B. *Enter the New Rule 41(b)*[228]

The use of the Internet to commit child pornography crimes has blurred traditional notions of jurisdiction. Recognizing this, all three branches of the federal government supported a change to the Federal Rules of Criminal Procedure.

But the Playpen NIT was deployed before the new Rule 41(b) took effect. Cases on the cusp of the rule change are divergent. Ultimately, those upholding the FBI's operation are both legally and justly correct.

1. The Playpen NIT Warrant Was Legally Sufficient under the Old Rule 41(b)

Even absent the new Rule 41(b), the Playpen NIT warrant was legally sufficient for a variety of reasons.

a. *NITs as "Tracking Devices"*

In *United States v. Matish*,[229] the court stressed that although the Playpen NIT was not a search, the warrant was valid because the NIT was sufficiently

---

Amendment is involved. . . . [Petitioner] was relying upon his misplaced confidence that [his false friend] would not reveal his wrongdoing.").

224 JOSHUA DRESSLER ET AL., 1 UNDERSTANDING CRIMINAL PROCEDURE § 6.05(B) (7th ed. 2017).

225 385 U.S. 293 (1966).

226 401 U.S. 745 (1971).

227 Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967). Anyway, there is no textual basis in the Constitution for this supposed right.

228 FED. R. CRIM. P. 41(b). The revised Rule took effect December 1, 2016.

229 193 F. Supp. 3d 585 (E.D. Va. 2016).

analogous to a tracking device, and thus, the magistrate did not exceed her authority under Rule 41(b)(4).[230] The court explained that, under the Rule, "[t]he tracking device must be installed within the magistrate judge's district, but the warrant 'may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both.'"[231] Consequently, the warrant "authorized the FBI to install a tracking device on each user's computer when that computer [virtually] entered the Eastern District of Virginia—the magistrate judge's district."[232]

The court cleverly espoused that "whenever someone entered Playpen, he or she made, in computer language, 'a virtual trip' via the Internet to Virginia, just as a person logging into a foreign website containing child pornography makes 'a virtual trip' overseas."[233] Buttressing this point, the court cited *Kyllo v. United States*,[234] which held that where "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'"[235] The court noted that the *Kyllo* "majority expressly rejected the dissent's attempts to distinguish 'off-the-wall' home surveillance and 'through-the-wall' observation."[236] The Supreme Court thus equated the government's electronic surveillance of a home via the thermal imaging device to actual boots-on-the-ground entry into the home.[237] Transposing the actors, the *Matish* court reasoned that "when users entered Playpen, they came into Virginia in an electronic manner, just as the police in *Kyllo* entered a home in an electronic manner."[238]

Therefore, because the NIT warrant complied with Rule 41(b)(4), the magistrate judge did not contravene Section 636 of the Federal Magistrates Act.[239]

b. *The Pending Rule Change Signaled that the Playpen NIT Warrant and Its Execution Were Valid*

In *United States v. Darby*,[240] the defendant unsuccessfully argued that nothing in Rule 41(b) authorized the magistrate judge to issue the NIT

---

230 *Id.* at 613.

231 *Id.* at 612 (quoting FED. R. CRIM. P. 41(b)(4)).

232 *Id.* at 613.

233 *Id.* at 612. *Contra* United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016).

234 533 U.S. 27 (2001).

235 *Matish*, 193 F. Supp. 3d at 613 (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)).

236 *Id.*

237 *Id.*

238 *Id.*

239 *Id.*

240 190 F. Supp. 3d 520 (E.D. Va. 2016).

warrant.[241] Because the NIT warrant allowed the government to use the NIT against any computer that logged into the Playpen website—and these computers could have been located anywhere in the world—the defendant alleged the magistrate violated Rule 41(b), which allows magistrates to issue warrants only for searches inside their districts or outside the district in very limited circumstances, which this was not.[242] The court disagreed, spotlighting the looming change to the Rule.

> The information gathered by the warrant was limited: primarily the IP addresses of those that accessed Playpen and additional information that would aid in identifying what computer accessed the site and what individual used that computer. Defendant seeks suppression because of an alleged violation of a Federal Rule of Criminal Procedure, *a rule that will likely be changed to allow explicitly this type of search. The pending amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes*. That is, there is nothing unreasonable about the scope of the warrant itself. *The FBI should be applauded for its actions in this case*.[243]

As to particularity and probable cause, although the warrant authorized the FBI to deploy the NIT at the point of log-in, the FBI deployed it in a much narrower fashion.[244] For instance, in *Matish*, the court highlighted that the FBI waited until the defendant took the extra step to click on a particular post. Specifically, he logged into Playpen, navigated to the bestiality section—which advertised prepubescent children engaged in sexual activities with animals—and clicked on the post titled "Girl 11YO, with dog."[245]

c. *Even If the Old Rule 41 Did Not Cover the NIT Warrant, Exclusion Is Unwarranted*

Matish recognized that although some sister courts held the tracking device provision inapplicable to the NIT warrant, many of those courts still upheld the warrant on other grounds.[246] For example, in *United States v. Werdene*,[247] the Eastern District of Pennsylvania held that although the magistrate judge in Virginia lacked authority, suppression was neither required nor appropriate.[248]

---

241 *Id.* at 534.

242 *Id.* at 534–35. Quoting the Federal Magistrates Act, 28 U.S.C. § 636(a)(1) (2012), the court held that the judge exercised authority that was "conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts." *Id.*

243 *Darby*, 190 F. Supp. 3d at 538 (emphasis added).

244 *Matish*, 193 F. Supp. 3d at 595.

245 *Id.*

246 *Id.* at 612.

247 188 F. Supp. 3d 431 (E.D. Pa. 2016).

248 *Id.* at 436.

The exclusionary rule was developed to deter police misconduct. Thus, when police officers show "deliberate, reckless, or grossly negligent" disregard for Fourth Amendment rights, the exclusion of evidence is warranted. But when police officers act with an objectively reasonable, good-faith belief in the lawfulness of their conduct, then the evidence should not be excluded because "there is no bad conduct to deter."[249] With this in mind, the First Circuit in *United States v. Levin*[250] held the Playpen NIT was lawful.[251] In reaching its decision, the court emphasized that "the government presented the magistrate judge with a request for a warrant, containing a detailed affidavit from an experienced officer, describing in detail its investigation, including how the NIT works, which places were to be searched, and which information was to be seized."[252] Moreover, the court suggested that any mistake in issuing the warrant was a mistake on the part of the magistrate judge, not the executing officers.[253] (In other words, the issue was not the *officers'* exceeding the scope of an appropriate warrant by *executing* it in an unlawful manner, but the *magistrate* exceeding the scope of her authority by *issuing* it.) The executing officers, after all, had no reason to suspect that a mistake had been made and the warrant was invalid, as this was the first time the issue of NIT warrants and their scope had been challenged.[254] Because there was no law enforcement conduct to deter, the First Circuit vacated the district court's decision to suppress the evidence discovered pursuant to both the NIT warrant and the warrant authorizing the search of Levin's computer. Not only did the court hold there was no conduct to deter, it further exclaimed that "such conduct should be *encouraged*" since it "leaves it to the courts to resolve novel legal issues," such as the ones raised in the case at bar (and here in this Comment).[255] To buttress its holding, the court noted that it was in good company, as the Eighth and Tenth Circuits had recently reached similar results.[256] Since then, other circuits have jumped on board, such as the Third, Fourth, and Sixth Circuits.[257]

---

249 INFORMER, *supra* note 126, at 12.

250 874 F.3d 316 (1st Cir. 2017).

251 *Id.* at 318.

252 *Id.* at 323.

253 *Id.*

254 *Id.*

255 *Id.*; *accord* INFORMER, *supra* note 126, at 12–13.

256 INFORMER, *supra* note 126, at 12–13 (citing United States v. Horton, 863 F.3d 1041 (8th Cir. 2017)); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017)).

257 *See, e.g.*, United States v. Tagg, 886 F.3d 579, 582 (6th Cir. 2018); United States v. Werdene, 883 F.3d 204, 207 (3d Cir. 2018); United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018).

2. Chicken Little, the Sky Is Not Falling: This Is Just About Magistrate Venue, Not a Grant of Carte Blanche Hacking Powers

The new Federal Rules of Criminal Procedure took effect December 1, 2016. Well-funded privacy groups are lamenting that the sky is falling due to an addition to Rule 41's *Venue for a Warrant Application*. Rule 41(b)(6)(A) now reads:

> At the request of a federal law enforcement officer or an attorney for the government . . .
>
> > (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
> >
> > > (A) the district where the media or information is located has been concealed through technological means . . . .[258]

With the rule change, law enforcement now has double-layered protection when seeking NIT warrants, should they be required: the tracking device provision ((b)(4)) and the new concealment provision ((b)(6)).

This change, advocated by federal and state law enforcement, adopted by the Supreme Court, and approved by Congress, is a major victory in the fight against child exploitation. All three branches of the government approve. Yet privacy advocates fear that it is the beginning of the end of the Fourth Amendment. This is simply not so. Contrary to the opponents' arguments, the venue modification does not unlawfully or unconstitutionally "confer new legal powers on the government."[259] Instead, the changes merely "loosen venue requirements, removing artificial geographical constraints" to a subset of warrants.[260] This same rationale was used back when the terrorism provision, Rule 41(b)(3), was created.[261]

---

258 FED. R. CRIM. P. 41(b).

259 Jonathan Keim, *Amendments to Federal Criminal Rule 41 Address Venue, Not Hacking Powers*, FEDERALIST SOC'Y (July 21, 2016), https://www.fed-soc.org/blog/detail/amendments-to-federal-criminal-rule-41-address-venue-not-hacking-powers.

260 *Id.*

261 A House Judiciary Committee report explained that the Patriot Act's amendment to § 2703 "does not affect the requirement for a search warrant" but instead was meant to decrease unnecessary investigative "delays caused by the cross-jurisdictional nature of the Internet." H.R. REP. NO. 107-236, pt. 1 at 57 (2001). To illustrate the unnecessary impediments of the (old) Rule 41: An investigator located in New York who is investigating a suspected terrorist in that city might have to seek a suspect's email from an ISP account located in California or cell tower data from a company located in Wichita. "The investigator would then need to coordinate with agents, prosecutors and judges in the district" in New York, California, and Kansas and obtain three individual warrants. These time delays are not mere inconvenience; rather, they "could be devastating to an investigation, especially where . . . terrorist acts are planned." *Id.*

"Privacy activists" in their crusade for privacy rights of the Playpen defendants neglect their own cause. What about the privacy rights of the child victims? These children no less have rights to the privacy and ownership of their own images, especially their naked bodies. These children also have profound interests in preserving their dignity. As Congress recognized, every viewing of child pornography represents a renewed violation of the privacy of the victims and repetition of their abuse.[262]

3. Meeting in the Middle

Although the Playpen NIT was not a search, obtaining a warrant is advisable.[263] If viewed through the *Jones* traditional trespass approach, a court could be persuaded that the NIT code extracting the IP/MAC address from the target computer was a trespass onto an "effect." Plus, Rule 41's venue provisions now greatly minimize law enforcement's burden in Dark Web–based child pornography cases.

The tension between liberty and security is at its apex as the Internet becomes a battlefield of its own. With that in mind, NITs must be reserved for a specific class of criminals.[264] Because nothing is immune from misuse, all three branches should take reasonably prudent measures to temper some of the constitutional concerns expressed by ICFT critics.[265]

For example, Congress should provide boundaries for NIT, similar to what it did with wiretapping after *Katz*. Guidelines could also include requirements for a semiannual report to Congress, which would include

---

262 Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 501(2)(D), 120 Stat. 587, 623 (2006) (congressional findings of 18 U.S.C. § 2251 note).

263 As in the case of Playpen, even if courts determine the NIT was a search, a warrant was used, and even if the warrant was defective, the *Leon* good-faith exception applies. *See, e.g.*, United States v. Levin, 874 F.3d 316, 324 (1st Cir. 2017).

264 NITs should never be so broad as to sweep up law-abiding citizens or used to target political opponents.

265 Congress must also ensure private party (like ISPs) compliance. The Court decided *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018), this last term, a decision that could have had a major impact on NIT if it went the other way. The initial question presented was whether a U.S. provider of email services must comply with a probable cause–based warrant issued under 18 U.S.C. § 2703 (2012) (Stored Communications Act) by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad. While this case was pending, Congress passed and the President signed into law the Clarifying Lawful Overseas Use of Data Act ("CLOUD"), Pub. L. 115-141 (2018), which directly addressed the issue before the Court. CLOUD amended the Stored Communications Act, to require email providers to disclose emails in their "possession, custody, or control," even if the emails are stored outside the United States. Soon thereafter, the government obtained and served Microsoft with a new warrant pursuant to CLOUD; the parties agreed that the new warrant had replaced the original warrant at issue in this case. In light of these facts, the Court concluded that because there was no longer any live dispute between the parties, the case was moot. *Microsoft Corp.*, 138 S. Ct. at 188.

statistics on successes and failures. The main point is to cabin arbitrary executive discretion, and not to require bureaucratic hurdle-jumping. At minimum, Congress and the Attorney General should develop standard operating procedures ("SOPs") for NIT execution. In addition to setting parameters, such SOPs could include provisions for oversight, such as by an agency's Office of Inspector General. As for the NIT *code*, the legislature could consider having a tech specialist in the judiciary who could verify the code is what the FBI purports it to be, and was executed as such. This could help mitigate some of defense counsel's concern when it is denied the code during discovery; it will similarly ensure that the particularity requirement of the warrant was met. Finding a rational balance between liberty and security must counsel the way ahead.

III. ENTRAPMENT IS AN UNVIABLE DEFENSE—THE PEDOPHILE IS PREDISPOSED; AN ELEMENTAL DEFENSE LIKEWISE DOES NOT WORK

The mere passive presence of a decoy site—a honeypot—does not rise to the level of solicitation.[266] It is extremely unlikely for someone to just stumble innocently upon a cache of child pornography.

In the ensuing litigation post–Operation Pacifier, several courts rightly quashed defendants' claims that (1) the NIT warrant was void for lack of probable cause and specificity as to them; and (2) the operation amounted to entrapment. The courts simply pointed to the nature of Playpen itself. As described in the affidavit, one had to take numerous affirmative steps to even find Playpen on Tor.[267] It is a stretch beyond imagination to think an innocent person would then register for Playpen.[268] The chances of innocence were even slimmer given that the homepage's logo featured lewd images of underage girls, and the preregistration page contained a warning to camouflage your identity.[269] All of this quashes an entrapment defense.

The Eastern District of Virginia in *Matish* held that it was reasonable for the magistrate judge to find that Playpen's focus on anonymity, coupled with its suggestive name, the provocative landing page logo, and the affidavit's description of Playpen's content (i.e., subforums that contained "the most egregious examples of child pornography and/or [were] dedicated to retellings of real world hands-on sexual abuse of children") constituted

---

266 In espionage, *honeypot* is a term of art for female spies masterfully skilled in seduction and betrayal. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 11:18, n.1 (2d ed. 2012). Colloquially, the human honeypot is modern-day "Bond girl." Entrapment concerns are much more palpable with these "Bond girls." As the song goes, "What you won't do for love . . ."

267 *Matish*, 193 F. Supp. 3d at 603.

268 *Id.* Afterall, it is clear that this was not a baby shower registry.

269 *Id.*

incontestable probable cause.[270] Similarly, the Western District of Washington in *United States v. Michaud*[271] asserted that "it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network."[272] This was particularly evident given that Michaud registered himself, spent over ninety-nine hours on the site, and accessed specific forums with disturbing titles.[273] These are not the actions of an innocent man.

Like the Eastern District of Virginia, the Eastern District of Wisconsin[274] and the District of Massachusetts[275] pointed to (1) "the complicated machinations through which users had to go to access the website"; (2) Playpen's suggestive name; (3) the landing page, which contained lewd images of underage girls and instructions for compressing large files (such as videos) for distribution; (4) the registration requirement; (5) the site's advising registrants to use fake email addresses and emphasizing the site's secretive nature; and (6) the fact that once a user completed all of *those* steps to become a registered user, the user had access to the entire site, which contained media that unequivocally depicted sexual acts of children—child pornography—and thus illegal contraband.[276] Accordingly, the courts concluded that any registered user must have been fully aware of the site's contents.[277] The courts further held that "the fact that one could become a registered user . . . and then view only information that did not contain illegal material, did not affect the probable cause determination."[278]

As these cases demonstrate, Playpen's users did not become users by happenchance or bad luck. At best, they assumed the risk; at worst, they were affirmative participants.

Relatedly, courts entertained and promptly quashed any entrapment defenses based on "outrageous" government conduct.[279] In *United States v. Kim*,[280] a Playpen defendant asserted that the FBI's two-week operation of the site constituted "outrageous" governmental conduct that violated due

---

270 *Id.* at 604 (alteration in original) (noting how sister courts, too, found this exact NIT warrant was supported by probable cause, citing, inter alia, *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269, at *1–2 (E.D. Wis. Mar. 14, 2016)).

271 No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

272 *Id.* at *5.

273 *Id.* at *2–3. For example, he "accessed a forum entitled 'Preteen videos—girls HC.' (HC stands for 'hardcore.')"

274 *Epich*, 2016 WL 953269.

275 United States v. Tran, 226 F. Supp. 3d 58, 67 (D. Mass. 2016).

276 *Epich*, 2016 WL 953269, at *1.

277 *Id.*

278 *Id.* at *1–2 ("[T]he mere existence of innocent explanations does not necessarily negate probable cause." (quoting United States v. Funches, 327 F.3d 582, 587 (7th Cir. 2003))).

279 Seminal entrapment cases include *Jacobson v. United States*, 503 U.S. 540 (1992); *United States v. Russell*, 411 U.S. 423 (1973); *Sherman v. United States*, 356 U.S. 369 (1957); and *Sorrells v. United States*, 287 U.S. 435 (1932).

280 No. 16-CR-191 (PKC), 2017 WL 394498 (E.D.N.Y. Jan. 27, 2017).

process and warranted dismissal of his indictment.[281] The court rightfully denied his motion,[282] saying:

> Defendant's due process claim boils down to the contention that the government's conduct was outrageous because the FBI could have accomplished its investigative goals without allowing for the actual distribution of child pornography and the attendant harm to the child victims. This argument, however, ignores, or at least gives short shrift to, the 'well-established' deference that is accorded to law enforcement in determining how to conduct its investigations. As the Second Circuit reminded us in *Al Kassar*, courts must give 'deference to the Government's choice of investigatory methods', and thus the burden for proving outrageous governmental conduct is a 'very heavy' one. Thus, the standard for demonstrating 'outrageous' governmental conduct is demanding for a reason.[283]

In other words, the government's conduct must "shock the conscience."[284] The only thing that shocked the conscience was defendant's own conduct.

The defendant in *United States v. Perdue*[285] met a similar fate. The Northern District of Texas held that the FBI's conduct was not so outrageous as to violate defendant's due process rights because (1) the FBI had secured a warrant; (2) the FBI did not create the website, alter its functionality, add content, or actively solicit new users; and (3) the defendant did more than provide meager assistance since he actively sought out the website, registered with a username and password, and downloaded specific images.[286]

Quite simply, the odious nature of child pornography removes any doubt that the defendant was predisposed—unlike narcotics, for instance. An otherwise lawful and moral person may be reasonably peer-pressured to smoke marijuana or think doing so will make him "cool." However, no one is "cool" if he sexually exploits a child. Indeed, society and hardcore felons[287] alike despise pedophiles.

And using an Internet avatar like Sweetie is not entrapment. Under the Sweetie "sting," a person had to complete two affirmative steps before he

---

281 *Id.* at *1.

282 *Id.*

283 *Id.* at *4 (citations omitted).

284 United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999); *see also* United States v. Ammons, No. 3:16-CR-00011-TBR, 2017 WL 4355670, at *4 (W.D. Ky. Sept. 29, 2017) ("The Court stands in good company in its decision to deny a motion [by a Playpen defendant] to dismiss an indictment based on an outrageous government conduct defense." (citing *United States v. Vortman*, No. 16-CR-210-THE-1, 2016 WL 7324987, at *1 (N.D. Cal. Dec. 16, 2016); *United States v. Hammond*, No. 16-CR-102-JD-1, 2016 WL 7157762, at *6 (N.D. Cal. Dec. 8, 2016); *United States v. Owens,* No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016); *United States v. Anzalone*, No. 15-10347-PBS, 2016 WL 6476939, at *5 (D. Mass. Oct. 28, 2016), *appeal docketed*, No. 17-1454 (1st Cir. May 5, 2017); *United States v. Allain*, No. 15-CR-10251, 2016 WL 5660452, at *13 (D. Mass. Sept. 29, 2016); *United States v. Chase*, No. 15:15-CR-00015-RLV-DCK-1, 2016 WL 4639182 at *2 (W.D.N.C. Sept. 6, 2016))).

285 237 F. Supp. 3d 471 (N.D. Tex. 2017).

286 *Id.* at 479–80.

287 The general notion is that pedophiles are the bottom-of-the-food-chain in prisons and are usually kept out of general population for their safety.

was considered a potential predator and before researchers began trying to identify him.[288] First, the predator had to approach Sweetie. The researchers never initiated the chats (in a way, it was a honeypot). Consistent with chatroom nomenclature, researchers used chat names that clearly indicated Sweetie's age (ten), gender (female), and location (Philippines). Therefore, there was no mistake that individuals who approached Sweetie were interested in interacting with a prepubescent girl. As a double layer of caution, researchers reminded individuals that they were chatting with a child. Those who proceeded sealed *their own* fate. They assumed the risk.

Second, the individual had to request or accept an offer to view a webcam sex show performed by ten-year-old Sweetie. Consistent with WCST business practice, Sweetie asked for payment to view the puppeted performance. Only after the individual made his deposit did researchers consider him a predator and begin working to identify him. The predators affirmatively attempted to engage in child exploitation by their own volitions.

Third, neither legal nor factual impossibility are viable defenses here. Sweetie's predators cannot claim they are not guilty because the "girl" Sweetie did not actually exist.[289] As discussed *supra* Section I.A.1.c., federal law prohibits obscene *virtual* child pornography. That which the predators attempted to do—sexually exploit a child; receive child pornography—*is* a crime. This is distinguishable from the classic legal impossibility example, where a person shoots a tree stump. The shooter cannot be guilty of attempted murder—one cannot "kill" a tree stump and the law does not proscribe killing a tree stump.

The other side of the coin is factual impossibility. Instead of firing shots into a tree stump, imagine the person fires shots into a room late at night thinking her intended target was asleep in bed. This *is* attempted murder even if the only thing to receive a gunshot wound is a pillow or teddy bear. So, like the teddy bear, it is irrelevant that the pedophile, in attempting to talk to a real prepubescent child, only interacted with an avatar.

Mistakes of fact must be honest and reasonable to be successful defenses or mitigation tactics.[290] For example, in *United States v. Cromitie*,[291] the defendant attempted to bomb several Jewish centers and a New York airport but was given fake explosives by an FBI informant.[292] Just because the bombs did not go "boom" did not mean he was allowed to avoid a terrorism

---

288 Predators included on the list had to be at least eighteen years of age.

289 *Cf.* United States v. Farner, 251 F.3d 510 (5th Cir. 2001) (declining to apply a legal impossibility defense to a defendant convicted of attempting to entice a minor to engage in sexual activity where the victim was actually an adult undercover agent).

290 "A mistake-of-fact defense relieves a person of criminal liability where a reasonable mistake of certain facts means that the person did not have the culpable mental state required for the commission of the offense." United States v. Bowling, 770 F.3d 1168, 1174 (7th Cir. 2014). For general intent crimes, mistakes of fact usually must be reasonable to be valid defenses. *Id.*

291 727 F.3d 194 (2d Cir. 2013).

292 *Id.* at 203.

conviction.[293] The defense's logic would be akin to a defendant in a drug case saying, "Well, yeah, I wanted cocaine, but I got gypped; what I *actually* received was ten packets worth of Splenda, so I'm not guilty." The intent is the same.[294]

Sweetie-type defendants also do not have a viable defense alleging that because Sweetie was an avatar, no actual child was *harmed* (distinguishing this from the elemental issue of existence). Although Sweetie does not harm a child in the production process, Congress found that virtual "materials threaten children in other, less direct, ways."[295] For example, pedophiles might use such virtual or cartoon materials to entice children to participate in sexual activity.[296] "[A] child who is reluctant to engage in sexual activity with an adult, or to pose for sexually explicit photographs, can sometimes be convinced by viewing depictions of other children 'having fun' participating in such activity."[297] Secondly, "pedophiles might 'whet their own sexual appetites' with the pornographic images, 'thereby increasing the creation and distribution of child pornography and the sexual abuse and exploitation of actual children.'"[298] Under these rationales, the harm stems from the content of the images; the means of production is a side issue.[299]

In sum, multilayered affirmative steps and the depraved nature of child pornography—"so obviously at odds with common decency"[300]—show that entrapment is wholly absent.

IV. BENEFITS: HONEYPOTS (AND OTHER ICFT) CAN HELP VICTIMS OBTAIN RESTITUTION OR PREVENT FURTHER VICTIMIZATION

This Part transitions to the benefits of honeypots, NITs, and avatars. ICFT's functioning as nuclear weapons to child pornography websites—blowing Playpen to smithereens, for example—is not their only benefit. ICFT are also justified as identity instruments, serving dual purposes of identifying both perpetrators and victims of child exploitation. For perpetrators, ICFT facilitate justice by identifying defendants throughout the criminal enterprise.

---

293 *Id.* at 227. Relatedly, his entrapment defense was similarly unsuccessful.

294 *Cf.* United States v. Malloy, 568 F.3d 166, 171 (4th Cir. 2009) (reasoning that Congress's failure to provide for a mistake-of-age affirmative defense in a child sexual exploitation statute signaled a lack of intent to provide such defense).

295 Ashcroft v. Free Speech Coalition, 535 U.S. 234, 242 (2002).

296 *Id.*

297 *Id.* at 241 (alteration in original) (quoting Congress's findings).

298 *Id.* (quoting Congress's findings).

299 *Id.* at 242 ("Congress identified a [third] problem created by computer-generated images: Their existence can make it harder to prosecute pornographers who do use real minors. As imaging technology improves . . . it becomes more difficult to prove that a particular picture was produced using actual children. To ensure that defendants possessing child pornography using real minors cannot evade prosecution, Congress extended the ban to virtual child pornography.")

300 United States v. Goff, 501 F.3d 250, 260 (3d Cir. 2007).

For victims, ICFT can discover and rescue child victims. Overarching both is identification for victim restitution purposes: we can know which defendants owe and which victims are owed. Additionally, ICFT are potential prevention devices: ICFT can prevent possessors of child pornography from becoming producers and physical abusers.

A. *Paroline: A Dreadful Decision; Honeypots and the Like: A Potential Antidote*

> Every day of my life I live in constant fear that someone will see my pictures and recognize me and that I will be humiliated all over again. It hurts me to know someone is looking at them—at me—when I was just a little girl being abused for the camera. I did not choose to be there, but now I am there forever in pictures that people are using to do sick things. I want it all erased. I want it all stopped. But I am powerless to stop it just like I was powerless to stop my uncle. . . . My life and my feelings are worse now because the crime has never really stopped and will never really stop. . . . It's like I am being abused over and over and over again.[301]

"Amy" was brutally raped by her uncle as an eight-year-old girl.[302] But it did not end there. He also recorded the rapes.[303] And he disseminated those recordings on the Internet.[304] Over 3200 pedophiles downloaded images of "Amy's" rape.[305] One such patron of this exploitation was defendant Doyle Randall Paroline.[306] For the harm of knowing that he and thousands of others had images of her rape, "Amy" sought damages, including costs to cover counseling, lost income, and attorney's fees.[307]

Paroline was a travesty. For one, it was a case of judicial activism against the legislature. Specifically, the U.S. Supreme Court ruled against the purpose and text of the mandatory restitution law for victims of child sexual exploitation—which commands that courts "shall direct" a defendant to pay the victim the "full amount" of her losses[308]—and instead engrafted its own supremely impracticable and ineffective rule. Worse, the case made it insurmountably difficult for child exploitation victims to obtain restitution. But

---

301 Paroline v. United States, 572 U.S. 434, 440–41 (2014) (statement of "Amy," the victim) (alterations in original).

302 *Id.*

303 *Id.*

304 *Id.*

305 Richard Wolf, *Supreme Court Weighs Restitution in Child Pornography Case*, USA TODAY (Jan. 22, 2014, 1:03 PM), https://www.usatoday.com/story/news/nation/2014/01/22/supreme-court-child-pornography-restitution/4774101/.

306 *Id.*

307 Paroline v. United States, 572 U.S. 434, 434 (2014).

308 18 U.S.C. § 2259 (2012). This statute directed courts to calculate restitution in the same way as under the Mandatory Victims Restitution Act of 1996 ("MVRA"), 18 U.S.C. § 3663A, a more generic mandatory restitution law. While MVRA supplies general restitution guidelines for many federal offenses, § 2259 is specific to crimes under Title 110—sexual exploitation and other abuse of children.

there is perhaps a silver lining: the decision can justify law enforcement's use of ICFT. These tools can help find additional defendants in both the demand and supply chains, which can give victims the causation and restitution they deserve.

1. The Holding

Justice Kennedy, in a 5–4 decision, held that restitution to "Amy," who was forced to produce child pornography as a prepubescent girl, was proper under 18 U.S.C. § 2259 only to the extent the defendant (who plead guilty to possessing child pornography of "Amy" and other children) was the proximate cause of her losses.[309] Although the Court noted that victims should be compensated and that defendants should be held accountable, it held defendants should only be liable for the consequences and gravity of their own conduct, not the conduct of others.[310] On the surface this may sound reasonable, but underneath, one realizes the holding is absurd.[311]

As Justice Sotomayor powerfully stated in her dissent, a but-for requirement "would preclude restitution to the victim of the typical child pornography offense for the nonsensical reason that the child has been victimized by too many."[312]

2. The Effect

> I am surprised and confused by the Court's decision today. I really don't understand where this leaves me and other victims who now have to live with trying to get restitution probably for the rest of our lives. The Supreme Court said we should keep going back to the district courts over and over again but that's what I have been doing for almost six years now. It's crazy that people keep committing this crime year after year and now victims like me have to keep reliving it year after year. I'm not sure how this decision helps anyone to really know if, when, and how restitution will ever be paid to kids and other victims of this endless crime. I see that the Court said I should get full restitution "someday," I just wonder when that day will be and how long I and Vicky and other victims will have to wait for justice.[313]

Paroline failed to implement the Congressional command that victims receive restitution for the "full amount" of their losses. "[T]he legal issues swirling around restitution decisions have real world consequences for real world people: the defendants who must pay the awards and the victims who

---

309 *Paroline*, 572 U.S. at 434, 448.

310 *Id.*

311 Not just in theory but in practice.

312 *Paroline*, 572 U.S. at 474 (Sotomayor, J., dissenting).

313 Paul Cassell, *The Crime Victim's Reaction to Today's Supreme Court Decision*, WASH. POST (Apr. 23, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/23/the-crime-victims-reaction-to-todays-supreme-court-decision/?utm_term=.97a84e1bb075 (quoting "Amy" after the Supreme Court released its *Paroline* decision).

need those payments."[314] Although large restitution awards could financially burden predators, the stark fact remains that these criminals had a binary choice: to commit the crime or not to commit the crime.[315] Because they voluntarily chose to commit crimes with serious financial repercussions, Professor Paul Cassell—and counsel for "Amy"— commented, "I am unsympathetic to any argument that they should be able to leave victims without full compensation."[316]

Despite *Paroline*'s "resolution," courts continue to grapple with the mess the Supreme Court left. No intelligible equation exists, theoretically or mathematically. Victims did not tie this Gordian knot—victims have sufficiently demonstrated their losses. Instead, courts are left to arbitrarily guess how to apportion those damages between defendants, as seen in *United States v. Crisostomi*.[317]

In *Crisostomi*, the district court had the daunting task of implementing the confusing *Paroline* rules for calculating restitution damages. Along with hundreds of images of other young girls, the defendant possessed forty-nine images and three videos of victim "Vicky" and two images of victim "Cindy."[318] Vicky's father raped her, vaginally and anally, and subjected her to oral sex and bondage.[319] He recorded these rapes; the videos and images were then widely circulated on the Internet.[320] The court was unsure whether the defendant ever reproduced or distributed any of the images, although in all likelihood, he did.[321] The court *was* sure of the well-documented past and future medical and legal needs of the victims.[322]

Nevertheless, even with the supposed guideposts of *Paroline*, the court admitted that it struggled to determine the proper restitution award.[323] Discussing some of the *Paroline* factors, the court said that while some were "determinable with some precision," others were essentially useless for being

---

314 Paul G. Cassell & James R. Marsh, *Full Restitution for Child Pornography Victims: The Supreme Court's Paroline Decision and the Need for a Congressional Response*, 13 OHIO ST. J. CRIM. L. 5, 34 (2015). *See also The Need for Improving Restitution for Victims of Child Pornography Crimes after* Paroline v. United States*: Hearing on S. 295 before the Subcomm. on Crime of the H. Judiciary Comm.* (March 19, 2015) (statement of Paul G. Cassell), https://judiciary.house.gov/wp-content/uploads/2016/02/Testimony-Cassell.pdf.

315 Indeed, the eggshell rule also comes to mind.

316 *Child Exploitation Restitution Following the* Paroline v. United Staes *Decision: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Judiciary Comm.*, 114th Cong. 77 (2015) (statement of Paul G. Cassell, Professor of Criminal Law, University of Utah College of Law). Mr. Cassell was counsel for Respondent "Amy."

317 31 F. Supp. 3d 361 (D.R.I. 2014).

318 *Id.* at 365.

319 United States v. Miltier, No. 2:15cr151, 2016 U.S. Dist. LEXIS 159606, at *2 (E.D. Va. Sept. 17, 2016), *aff'd*, 882 F.3d 81 (4th Cir. 2018).

320 *Id.*

321 *Crisostomi*, 31 F. Supp. 3d at 364–65.

322 *Id.* at 364.

323 *Id.*

"virtually unknown and unknowable, regardless of the detail available in the record."[324] In other words, a judge is left to guesstimate or throw blindly at an unknown target: how is a district judge supposed to make a reliable estimate of the scope of the defendant pool when even the Supreme Court admits "most [offenders] will, of course, never be caught, or convicted?"[325] Calling such calculations difficult at best, and at worst impossible, the court expressed that it was not "comfortable making such calculations" but believed it was "compelled to do so" by *Paroline*.[326]

In calculating Vicky's losses, the court endeavored to make a "*reasonable assumption* [of] the number of people caught, convicted, and ordered to contribute to [Vicky's damages]," a feat in itself.[327] Given that there were approximately 500 known offenders, the court estimated that number "could double to an additional 1,000 offenders."[328] Applying the *Paroline* factors, the court thus determined that the defendant was responsible for 0.1 percent (1/1000) of Vicky's remaining losses, so it granted her a pitiful $713.68.[329]

As for Cindy, the court acknowledged that a similar figure for her damages was not available.[330] Thus, it decided to apply a proportionality assessment.[331] The court arbitrarily estimated that 53 percent of Cindy's damages were remaining.[332] Like Vicky, the court speculated that there might be 1000 more offenders caught, convicted, and made to pay restitution, making the defendant only 0.1 percent responsible.[333] The court awarded her a measly $683.41.[334]

Another federal court wrestling with *Paroline*'s wake awarded "Vicky" a mere $407.05 of the reasonable $10,000 she asked for, under a slightly different framework from *Crisostomi*.[335] Under *Crisostomi*, however, she would have been awarded only approximately $200.[336]

Shockingly, some courts interpret § 2259 and *Paroline* to mean that the defendant is responsible only for the "tangible, monetary losses" incurred

---

324 *Id.*

325 *Id.* (quoting Paroline v. United States, 572 U.S. 434, 460 (2014)).

326 *Crisostomi*, 31 F. Supp. 3d at 364.

327 *Id.* at 365 (emphasis added).

328 *Id.*

329 *Id.*

330 *Id.*

331 *Id.*

332 *Crisostomi*, 31 F. Supp. 3d at 365.

333 *Id.*

334 *Id.*

335 United States v. Miltier, No. 2:15cr151, U.S. Dist. LEXIS 159606, at *14–15 (E.D. Va. Sept. 17, 2016), *aff'd*, 882 F.3d 81 (4th Cir. 2018).

336 *Id.*

and not the nonpecuniary harm or loss caused.[337] In essence, victims of car accidents or slip-and-falls have better chances of recovery.

These are just a small sample of cases that expose the difficulties lower courts have faced after *Paroline* and will continue to face if Congress does not intervene. With no clear methodology, calculations are often arbitrary and completely speculative, resulting in pathetic payouts. Such monetary values serve no deterrence purposes and are a slap in the face to child victims.

The absurdity of the *Paroline* holding is seen in the comparable sex-trafficking context. The Trafficking Victims Protection Act ("TVPA") makes restitution mandatory in sex-trafficking cases.[338] Arguably simpler than § 2259, the TVPA methodology requires recovery of "the greater of the gross income or value to the defendant of the victim's services or labor" under the Fair Labor Standards Act.[339] Nevertheless, over half the time, prosecutors inexplicably do not seek restitution at all.[340] And even a decade after its passage, courts still stumble when implementing the TVPA's restitution provision. Despite the TVPA's mandatory restitution requirement, a recent study found that restitution was awarded in only 36 percent of cases nationally.[341]

Congress's wishes and victims' needs are not being met. Now is the time to make mandatory mean mandatory; the justice system must enforce what is mandatory and transfer predators' ill-gotten gains to victims to make them (as) whole (as possible).

3. The Fix

The natural question arises, "But how is a child victim supposed to identify all the pedophiles who viewed her exploitation?" This is a tremendously heavy burden to place on the victim, and this burden is virtually impossible to overcome given the clandestine nature of the child pornography enterprise. Such requirements are unrealistic. This has the effect of shortchanging victims who did nothing wrong and in no way were legally or morally culpable. The burden must be placed on the defendant. Doing so will incentivize a defendant to rat out his other pedophile cohorts to indemnify him for the dues owed.

---

337 United States v. Galan, No. 6:11-cr-60148-AA, 2014 U.S. Dist. LEXIS 94377, at *10 (D. Or. July 11, 2014), *rev'd on other grounds*, 804 F.3d 1287 (9th Cir. 2015)).

338 18 U.S.C. § 1593 (2012).

339 *Id.*

340 Alexandra F. Levy & Martina E. Vandenberg, *When "Mandatory" Does Not Mean Mandatory: Failure to Obtain Criminal Restitution in Federal Prosecution of Human Trafficking Cases in the United States*, HUMAN TRAFFICKING PRO BONO LEGAL CENTER 15, http://www.htprobono.org/wp-content/uploads/2014/09/HTProBono-Trafficking-Restitution-Report.pdf (last visited Aug. 25, 2018) (noting that in 2014, the DOJ prosecuted 113 sex traffickers (of adults and children), and that despite the TVPA's requirements, restitution was only awarded in 36 percent of cases).

341 18 U.S.C. § 1593.

In response to the disastrous *Paroline* decision, the Senate, led by senators on both sides of the aisle (namely, Senators Hatch (R-Utah) and Schumer (D-N.Y.)) and backed by forty-four state attorneys general, introduced a bill to strengthen the law for child pornography victims: The Amy and Vicky Child Pornography Victim Restitution Improvement Act of 2015.[342] Reflecting the nature of these horrendous crimes, the Act does three things: (1) it considers the total harm to the victim, including from individuals who may not yet have been identified; (2) it requires real and timely restitution; and, (3) it allows defendants who have contributed to the same victim's harm to spread the restitution cost amongst themselves.[343]

In describing the purpose of the Act, Senator Hatch aptly announced, "Victims of child pornography suffer a unique kind of harm and deserve a unique restitution process."[344] Senator Schumer added, "The tragic effect of the Supreme Court's decision in *Paroline* was this: the more widely viewed the pornographic image of a victim, and the more offenders there are, the more difficult it is for the victim to recover for her anguish and her damages. But there should not be safety in numbers."[345] The bill passed 98–0.[346]

If one parses the *Paroline* majority's and Justice Sotomayor's views closely, a two-part fix emerges: Congress should (1) enact a federal rule of contribution among child pornography defendants; and (2) replace "proximate cause" with "aggregate causation."[347] Doing so would make it possible for the Amys of the world to obtain full restitution from even one perpetrator in the sordid marketplace. The fix incentivizes the current debtor-defendant to identify others as contributors. In other words, let the defendant go after his peers in the market to foot some of his bill. This economic incentive also results in a benefit for law enforcement, as it identifies other coconspirators or the kingpins. Another advantage of this solution is that it minimizes the restitution, even if levied against a single person, from being coined an excessive personal fine. Finally, this solution puts the burden of parsing out blame on the guilty criminal, where it belongs, and not on the child who never asked to be on the Internet in the first place.

---

342 S. 295, 114th Cong. (2015) (as passed by Senate, Feb. 12, 2015). The UK maintains similar laws. *See* Jane Fae, *UK to Outlaw Cartoons of Child Sexual Abuse*, THE REGISTER, https://www.theregister.co.uk/2008/05/28/government_outlaws_pictures/ (May 28, 2008, 9:13 AM).

343 S. 295.

344 Press Release, In Response to Recent Supreme Court Decision, Senators Hatch and Schumer to Introduce Bill to Strengthen the Law for Child Pornography Victims (May 7, 2014), https://www.hatch.senate.gov/public/index.cfm/releases?ID=b82cec32-bec4-485c-aba2-ac9d43c5d456.

345 *Id.*

346 161 CONG. REC. S917, 920 (daily ed. Feb. 11, 2015). Although the Senate passed the bill, the bill did not pass the House of Representatives in the 114th Congress. The Senate rejuvenated the bill by unanimously passing the bipartisan Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2017 (S. 2152). That bill now sits on the desks of the House Judiciary Committee.

347 Dean A. Mazzone, Paroline v. United States: *The Question of Restitution*, 16 ENGAGE, July 15, 2015, at 28, 29, https://fedsoc-cms-public.s3.amazonaws.com/update/pdf/AckJSXWz655lr5Qg9zp18w40KcB8r8gtFkSBrQ01.pdf.

Regardless of the specific legislative or interpretive fix, honeypots and other ICFTs are solutions. In sum, ICFT can help both law enforcement and defendants identify other predators, thereby pruning courts' arbitrary and speculative restitution calculations. ICFT's ability to identify defendants can prevent them from shirking their responsibilities under § 2259 to pay the *innocent* victims the restitution they deserve.

B. *ICFT Can Prevent Users from Becoming Abusers*

Many viewers of child pornography eventually molest children or are already doing so. Emboldened viewers become producers. Honeypots, Sweetie, and NITs have the power to potentially prevent audience members from becoming lead actors or directors.

Habitually viewing child pornography results in the viewer becoming desensitized to the abuse behind the camera.[348] This desensitization is one potential trigger that leads to physical abuse.[349] The viewer does not appreciate the gravity of his actions and may misperceive the child pornography as just some make-believe fantasyland or some actor in a Hollywood movie—not a real-life child, someone's son or daughter, being molested. The viewer is thus prone to escalate from eyes-only to hands-on.

Some critics argue that "not all pedophiles become child molesters," which is true.[350] Critics also argue that just because "pedophiles use child pornography to become sexually aroused . . . does not translate into sexual abuse,"[351] which is untrue. Conceding, as they must, that consumption of child pornography correlates with crimes against children, some critics reason that such correlation alone does not necessarily imply causation.[352] But the mere existence of child pornography *is child abuse*. A child was abused by its creation. That child is further abused as the image or video is circulated and viewed again and again. Although watching child pornography does not always lead to the viewer becoming a molester, he is a vicarious molester. So even if the premise is true that perfect statistical causation does not exist, it still does not support the inference that child pornography is a necessary evil, or victimless, or that the viewer is just an innocent spectator. Without the demand, there would be nearly no supply (and vice versa). In other words, going backwards, child pornography producers—those molesting children and memorializing it—create child pornography for other likeminded pedophiles. Those other pedophiles may get the grand idea that they, too, can

---

348 *See* H.R. Rep. No. 104-358, at 13 (1996).

349 The emphasis here is on *child*, not adult, pornography.

350 Debra D. Burke, *The Criminalization of Virtual Child Pornography: A Constitutional Question*, 34 HARV. J. ON LEGIS. 439, 464 (1997).

351 *Id.*

352 *Id.* at 464–65.

create their own videos, whetting their sexual appetite, and gaining notoriety and money along the way. A triple threat. Using ICFT to shut down these Dark Web theatres may erase the incentive or at least act as a strong deterrent.

Critics also contend that "pedophilia is a complicated disorder lacking a simple explanation for its cause."[353] And because of this, "to assume that child pornography causes pedophiles to molest children, and to suggest that child pornography be eradicated as a solution to such criminal behavior, is too simplistic a response."[354] First, exploring and explaining why pedophiles do what they do may be an interesting topic for psychologists, but the law is concerned with preventing crime and seeking justice, especially for such defenseless victims. Undoubtedly, behavioral science is beneficial to profile and catch unknown serial killers, for example. But in the child pornography context, the "why" is less important, because of the nature of the crime and, as discussed in this Comment's introduction, because the perpetrators span all walks of life. So is the solution simplistic? No. Simple? The solution itself, yes, but the implementation is more complicated. Honeypots and NITs can help make the solution more attainable. Second, the enterprise of child pornography is by its very nature child exploitation and is created by molesting children. Whether it is the chicken or the egg does not matter; it must be stopped. The simple fact is that child pornography makes the initial molestation continue in perpetuity.

The rare bird who uses child pornography to keep a lid on his physical-molestation desires does not expunge the majority who actually molest, does not justify child pornography's existence, and does not erase the simple fact that child pornography is definitionally exploitation. True, those who enjoy watching sadomasochist adult pornography are not ipso facto violent rapists. It is entirely plausible that someone who enjoys violent adult pornography uses it as an outlet so as to not manifest such fantasies through violent rape. But there are fundamental differences between adult and child pornography. Adult pornography is not a crime. Child pornography is. Adult pornography (generally) stars consenting adults. Child pornography never does.

Indeed, many child pornography possessors are what experts term "dual offenders," meaning they not only possess child pornography, but they actually physically sexually abuse children.[355] Factoring in those who attempt physical sexual victimization, over half of possessors are dual offenders.[356]

To support the idea that any connection between pedophilia and contact sex offending is "merely implied," one critic noted a court that blamed social forces, arguing that the Internet made it easier for someone to create a collection and that "as the popular culture has become more and more saturated with a debased concept of human sexuality, this natural aversion in many

---

353 Burke, *supra* note 350, at 464 n.154.

354 *Id.*

355 WOLAK ET AL., *supra* note 41, at 16 (concluding that 40 percent are dual offenders).

356 *Id.*

people [concerning child pornography] seems to have grown weaker."[357] But that is precisely why law enforcement should use ICFT and stop child pornography's growth. Society's aversion purportedly becomes weaker, pedophiles get bolder, and the children get younger and more tortured. Labeling child pornography a "cathartic outlet" disturbingly misses the point that children were victimized. The child's experience was the complete opposite of cathartic; it was a life-altering crime.

Critics of the current sentencing framework for child pornography offenders question Congress's impetus behind its stance—namely, the underlying presumption that child pornography offenders are undetected child molesters.[358] These critics believe it is mostly a farce, oddly calling it a "moral panic."[359] To buttress this point, one critic points to a purported "growing number of federal judges [who] instead view most offenders who possess or trade child pornography as mostly harmless to others."[360] That is practical nonsense. Admittedly, anyone could find or generate a study that suits one's conclusion—the stance this Comment advocates included. Nevertheless, the "mostly harmless to others" retort is fundamentally flawed. Such falsehood is demonstrated as one considers several incontestable facts:

(1) The sheer volume of child pornography available on the Internet, meaning a mass quantity of child victims;

(2) The number of predators accessing it, which increases the demand for more child pornography. Consequently, this increases (a) the quantity of new victims, (b) the quantity of new material of current victims, and (c) a deepened "quality" of harm to those victims knowing their abuse is widely circulated;

(3) The desensitizing of predators. The "virtual" nature of child pornography numbs the viewer, as if it is a work of fiction. Furthermore, perpetrators of online child sexual abuse justify their aberrations by joining online peer groups with similar interests and persuasive tendencies.[361]

---

357 Hamilton, *supra* note 2, at 570–71 (alteration in original) (quoting United States v. Ontiveros, No. 07-CR-333, 2008 U.S. Dist. LEXIS 58774, at *17 (E.D. Wis. July 24, 2008))

358 Although punishment and sentencing are outside the scope of this Comment, the critics' rationales are worth mentioning and fit here. I do agree with some of the critics that the current sentencing guidelines are sometimes oblivious to the differences between child pornography offenders. For example, a fifty-year-old man who receives a photograph of a prepubescent girl actually being sodomized by a middle-aged man should not be assigned the same base offense level for sentencing as would an eighteen-year-old who engages in sexting and sends a same-aged friend a consensually taken, nude photo of a seventeen-year-old girlfriend. Hamilton, *supra* note 2, at 546.

359 *Id.* at 547.

360 *Id.* at 545 (citing one "Sixth" Circuit case (it is an Eighth Circuit case)).

361 Discussed *supra* Section I.A.1.a.

(4) Predators acting as cheerleaders. Virtual peer groups (really, coconspirators to a crime) encourage more abuse and more victims—either directly, by saying they want more videos of "Child A", or indirectly, through the desensitization discussed in factor (3), which spawns abuse of new victims: Child B, C, D, etc.

(5) The backdrop that child exploitation victims are becoming increasingly *younger* and their abuse increasingly *more violent, sadistic, and deranged*.[362]

(6) The pain and suffering the individual child experiences.[363] Certainly, the child's parents, too, agonize knowing that their son or daughter was victim to such malevolent crimes.

(7) Relatedly, the failure of negative inferences. The presumption that because of the number of children a pedophile *did not* harm somehow lessons the harm to the child victim is erroneous. A heroin addict is mostly harmless to others. He injects himself with toxins. A one-time murderer may be mostly harmless to others. Still, the murderer must serve time for her crime, and the number of people she left alive does not in any way lessen the impact on her victim or the victim's family. Additionally, recidivism rates are highest for sex offenders.

To show that child pornography possessors are not molesters, critics note that having no prior criminal history is a predominant reason why judges reduce their culpability and sentence.[364] Perhaps that is because the possessors were *caught before the opportunity* arose to physically molest a child. Et voila, another justification for ICFTs.

In an effort to either minimize blameworthiness or to show "consensus" of feeling sorry for perpetrators, one critic provides the following description of the apparent perception of "many" federal judges: "We have had quite a number of people that are very similarly situated to [defendant], successful, hardworking, family people that get caught up in this."[365] The case from

---

362 Discussed *supra* Section I.A.1.a.

363 Discussed *supra* Section I.A.1.d.

364 Hamilton, *supra* note 2, at 562.

365 *Id.* at 545 (quoting United States v. Bain, 586 F.3d 634, 642 ([8]th Cir. 2009)) (alteration in original). The citation is incorrect and perhaps taken out of context. The quote is from the district court below, which concluded that it is "important . . . to promote *consistency* among those sentences." *Bain*, 586 F.3d at 642 (emphasis added). In any event, the circuit court affirmed Bain's sentence as substantively reasonable. The district court also said to Bain, "[Y]ou're going to pay dearly, your wife is going to pay dearly, everybody associated with you is going to pay dearly and it is painful because you were by all accounts very successful, a contributing member to your community, certainly to your workplace, it is

which that quote was taken, *United States v. Bain*,[366] involved the following set of facts: the FBI had received a tip from the Norwegian government on which it then executed a search warrant at Bain's house. There, they "seized three computers and numerous floppy disks containing 496 images and digital movies depicting minors engaged in sexual acts."[367] Bain admitted that he traded child pornography files from his home using the file sharing program Kazaa.[368] Although, overall, Bain was still sentenced to "the low end" of the Guidelines range, his base level sentence was *increased* because of several aggravating factors: (1) age: some of the victims were under twelve; (2) subject matter: some material portrayed sadism, masochism, or other depictions of violence; (3) distribution: he traded the material for more child pornography; (4) vehicle: he used a computer to receive and distribute material; and (5) quantity: the offense involved more than 600 images.[369] It is hard to imagine how Bain would have just stumbled upon child pornography or that his family-man status excuses his behavior. He got "caught up" in it because he is a freewill agent who chose to do so.

To further support her proposition, the critic cited a dissenting judge who oddly analogized child pornography cases to the thirteenth-century witch trials and burnings.[370] (The obvious retort is that the "witches" were victims, not perpetrators.) Remarkably, the defendant in that case (in addition to having almost 4000 still images, not counting the videotapes, in his garage alone—as well as digital images he downloaded on his computer from websites known to traffic child pornography) *molested* his son's friend.[371] The court below highlighted that the defendant "demonstrated no 'empathy, emotion, sorrow, compassion for those children, those thousands of children that are put in this position by people in a place of trust.'"[372]

The Third Circuit in *United States v. Goff*[373] provides an outstanding summary of the child pornography problem.

---

harsh." *Id.* at 640 (alteration in original). The circuit court stated, "It is unclear whether the district court meant the sentence was harsh, or whether the district court meant it was unfortunate that an otherwise well-functioning member of society had committed this crime." *Id.* In the end, the circuit court interpreted it as the latter, finding the sentence reasonable. *Bain*, 586 F.3d at 640–42.

366 586 F.3d 634 (8th Cir. 2009).

367 *Id.* at 636.

368 *Id.*

369 *Id.* at 635 n.3, 636, 640. As the court explained, although "only" 496 raw images were found, at least eight were video clips; video clips are assigned a sentencing value of seventy-five images each. *See* U.S.S.G. § 2G2.2 cmt. 6(B)(ii).

370 Hamilton, *supra* note 2, at 561.

371 United States v. Paull, 551 F.3d 516, 519, 521 (6th Cir. 2009) (quoting the court below) (this case did not address the defendant's being convicted with molestation; for purposes of sentencing, it was found based on a preponderance of evidence including the victim coming forward and substantial corroborating evidence).

372 *Id.* at 519, 521.

373 501 F.3d 250, 251, 258–260 (3d Cir. 2007).

> Goff has attempted to downplay the nature and seriousness of his crime, arguing that he was simply a "curious, casual user" of the child pornography website, and implying that his was a victimless crime because viewing the pornography was "a solitary, private activity of short duration driven by Mr. Goff's curiosity of the subject." His attorney made similar statements at the sentencing hearing. ("If the anonymous interaction with a far away [I]nternet wasn't possible, this may never even have happened. But where you have the ability to all by yourself, without involving another human being, sit at your computer and bring up the images that you want to look at, he violated the statute"; "he succumbed to this urge or whatever it was, to look at the images all by himself in his room"; "what he did alone in his house, all by himself, not involving another human being, just the computer screen"). In the letter he submitted to the District Court before sentencing, Goff emphasized this point, saying, "no one else was involved at any time." The district court appears to have accepted this line of reasoning. Interrupting the prosecutor's argument that possession of child pornography is "a serious matter and should be punished seriously," the court commented, "but it's truly a psychological crime. It is not a taking crime. Almost one might say a psychiatric crime."
>
> The briefest of forays into Goff's on-line fantasy world gives the lie to his cant about "solitary" activities and exposes the basic flaw in the District Court's implied conclusion that nothing wrong was going on here except in Goff's mind. According to the presentence report, one of the images is of "an adult male performing oral sex on a prepubescent female." The report goes on to describe, in detail we will spare readers, what is visible in the picture, as well as details of other examples from the hundreds of pictures Goff had paid for over time. *Children are exploited, molested, and raped for the prurient pleasure of Goff and others who support suppliers of child pornography. These small victims may rank as "no one else" in Goff's mind, but they do indeed exist outside his mind. Their injuries and the taking of their innocence are all too real. There is nothing "casual" or theoretical about the scars they will bear from being abused for Goff's advantage.* Far from persuading us that Goff's crime was relatively minor, his efforts to downplay the harm his actions have inflicted on others serve chiefly to highlight the concern the District Court should have had with Goff's failure to appreciate the seriousness of his offense.
>
> Similarly, Goff should not have gained any ground at sentencing by claiming, through his psychiatrist, that he has "never acted out in any sexual way with children." He was not charged with molestation, so pointing out that he hadn't committed it is, in one sense, irrelevant. In another more important sense, however, it does say something meaningful, albeit not what the defense intended. While the defense effort to draw a spectator-vs.-participant distinction does not show that Goff's pornography crime was of less than ordinary severity, it does reemphasize that Goff failed to fully appreciate that severity. *The simple fact that the images have been disseminated perpetuates the abuse initiated by the producer of the materials.* "The materials produced are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation." *New York v. Ferber*, 458 U.S. 747, 759 [1982]. *Consumers such as Goff who "merely" or "passively" receive or possess child pornography directly contribute to this continuing victimization. Having paid others to "act out" for him, the victims are no less damaged for his having remained safely at home, and his voyeurism has actively contributed to a tide of depravity that Congress, expressing the will of our nation, has condemned in the strongest terms.*
>
> In addition the consumer of child pornography "creates a market" for the abuse by providing an economic motive for creating and distributing the materials. In *United States v. Ketcham*, 80 F.3d 789, 793 (3d Cir. 1996), we explained that Congress's criminalization of the mere possession of child pornography "discourages its production by depriving would-be producers of a market." [374]

Empirics and studies aside, basic common sense renders ICFT imperative in the fight to protect children from sexual exploitation. A *Minority Report* argument has no place here. Rather, by swiftly catching child pornography viewers and bringing them to justice for those crimes, they may be

---

374 United States v. Goff, 501 F.3d 250, 251, 258–260 (3d Cir. 2007) (emphases added) (footnotes omitted) (most citations omitted) (minor punctuation changes made).

prevented from molesting children in the future or stopped from presently molesting children. ICFT are the means to that end. ICFT may solve unsolved crimes either through identifying the perpetrator or by identifying a silenced or unknown victim.[375]

CONCLUSION

Cruelty, like every other vice, requires no motive outside itself—it only requires opportunity.[376] The rape of a child is manifestly cruel. The recording, sharing, and viewing of the rape is similarly cruel. Child pornography is cruelty. Whether the motive is financial or sexual is irrelevant. Eliminating the *opportunity* is what matters. The quintessential way to do so is through ICFT.

Although the Dark Web absolutely has legitimate uses, it should not be the Wild West in which pedophiles can abuse children and roam free with impunity. Luckily there is a new sheriff in town, and he has arrived with a very effective lasso. The FBI's ingenuity with honeypots and NITs proved successful in Operation Pacifier, the bulldozing of Playpen. Although controversial, it was constitutional. The government must adopt and support such proactive investigative techniques. And, if given the opportunity, the U.S. Supreme Court should resolve the circuit split in the FBI's favor. Doing so will provide a deterrent effect by instilling in predators a fear of being caught and punished. As the sordid child pornography enterprise is on the cutting-edge, it would be irresponsible to force law enforcement to use antiquated relics. Likewise, it is unreasonable to expect law enforcement to sit and twiddle their thumbs in anticipation that a predator will deliberately reveal himself like Mark Salling did.

This Comment discussed "Concerns" and "Benefits." It examined concerns such as Fourth Amendment and entrapment issues and concluded they are not concerns after all. But it offered potential compromises to temper some of the concerns. The Comment then discussed the perhaps not-so-obvious benefits of ICFT. ICFT can identify other "unknown" perpetrators to help victims get the restitution they need, deserve, and are statutorily owed. These tools also may serve a prevention role, by stopping child pornography viewers from becoming producers and physical abusers.

It is not constitutional heresy to contend that if criminals can become better criminals through technology, law enforcement should similarly leverage technology to become better crime fighters. The sexual exploitation of a child is a unique crime, and such moral depravity must be met with subzero tolerance and top-of-the-line investigative tools. Honeypots, NITs, and

---

375 Desirae Krislie C. Tongco, Note, *Saying No to "Cutting Corners": The Military Courts' Correctness in Rejecting the Use of Evidence of Sexual Assault Against a Minor to Search for Child Pornography*, 60 HOWARD L.J. 593 (2017) (providing a summary of studies that show a correlation and those that are not so clear).

376 ELIOT, *supra* note 1.

Sweetie are critical tools in the law enforcement toolkit, and they are necessary for fighting the evils of child pornography.

You catch more bees with Sweet honey.