NOTE

You Don't Have Mail: The Permissibility of Internet-Use Bans in Child Pornography Cases and the Need for Uniformity Across the Circuits

*Sam Cowin**

ABSTRACT

The federal courts of appeal have formed vastly different conclusions with respect to the reasonableness of Internet-use bans as a term of supervised release in virtual child pornography cases. All courts ground their decisions in 18 U.S.C. § 3583(d), the federal statute governing supervised release conditions. Nonetheless, when presented with seemingly analogous facts, some courts uphold Internet-use bans, whereas others strike them down. Courts upholding such bans conclude that they constitute effective deterrents and ensure public safety. Courts overturning the bans, on the other hand, assert that they unreasonably deprive offenders of their liberty interests.

Because decisions regarding the permissibility of Internet-use bans are, under the current statutory regime, incoherent at best and arbitrary at worst, Congress should amend § 3583(d) to provide judges with meaningful, cyber-specific guidance. Accordingly, this Note proposes that Congress adopt the UNIFORM Act, which sets forth child pornography–specific guidelines for

* J.D., expected May 2012, The George Washington University Law School; B.S., 2008, University of Illinois. I would like to extend my appreciation to everyone who provided feedback on this Note. In particular, I would like to thank Alex Hastings, Brian Thavarajah, Brittany Warren, and Richard Crudo. Many thanks, as well, to my law school friends, colleagues, and professors who made the last three years so enjoyable: Mike Lanning, Alec Stone, Devin Anderson, Sam Quatromoni, and Professors Burlette Carter and Peter Smith. Finally, and most importantly, thanks to my family who supported me during law school: Lauren, Dad, Mom, "the brothers," Saly, Harv and Bob, Nana, and of course, Zimm the dog.

determining the terms for supervised release. Inspired by the United States Sentencing Guidelines and extracted from the caselaw regarding the permissibility of Internet-use bans, the UNIFORM Act seeks to limit judges' sentencing discretion in child pornography cases. At bottom, this Note posits a commonsense compromise, informed by existing statutes and caselaw, which would achieve consistency in an area of the law currently plagued by judicial ambiguity.

TABLE OF CONTENTS

INTRODUCTION

On May 13, 2002, Karl Zinn visited what he believed was a pornographic video website and expressed interest in purchasing videos depicting girls between the ages of six and thirteen.[1] Little did Zinn know, the website, operated by the U.S. Customs Service, was part of an undercover government sting operation targeting child pornography offenders.[2] Upon choosing two child pornography videos for purchase, Zinn received an order form, which he subsequently completed and mailed to the website operators.[3] Approximately two weeks later, Zinn received the videos in the mail as part of a controlled government delivery.[4] Hours later, U.S. Customs agents executed a search warrant of Zinn's home and recovered computer storage devices containing thousands of child pornography images.[5] Zinn ultimately pled guilty to possessing materials containing images of child pornography.[6]

The district court sentenced Zinn to a thirty-three-month prison term, followed by three years of supervised release.[7] As a term of Zinn's release, the court prohibited him from using the Internet without prior permission from his parole officer ("PO").[8] On appeal, the Eleventh Circuit upheld the permissibility of the Internet-use restriction.[9]

Gregory Sofsky, on the other hand, collected child pornography images procured primarily over the Internet.[10] Sofsky's hobby, however, constituted more than mere collection. Indeed, in addition to storing child pornography on his home computer, Sofsky used the In-

1 United States v. Zinn, 321 F.3d 1084, 1086 (11th Cir. 2003).
2 *Id.*
3 *Id.*
4 *Id.*
5 *Id.*
6 *Id.* (holding that Zinn had violated 18 U.S.C. § 2252A(a)(5)(B) (2006)).
7 *Id.*
8 *Id.* at 1087.
9 *Id.* at 1093.
10 United States v. Sofsky, 287 F.3d 122, 124 (2d Cir. 2002).

ternet to exchange child pornography images with other like-minded individuals.[11] After monitoring Sofsky's Internet activity, the government executed a search warrant on his home, and agents discovered more than 1000 images of child pornography.[12] Sofsky ultimately pled guilty to receiving child pornography.[13]

As was the case in *United States v. Zinn*,[14] the district court sentenced Sofsky to time in prison, followed by a period of supervised release.[15] As a condition of Sofsky's supervised release, the court prohibited him from using the Internet without approval from his PO.[16] On appeal, however, the Second Circuit came to a very different conclusion than the *Zinn* court with regard to the permissibility of Internet-use restrictions.[17] Noting that "[c]omputers and Internet access have become virtually indispensable in the modern world of communications and information gathering," the court held that the Internet-use ban at issue was impermissible.[18]

Presented with two seemingly analogous virtual child pornography cases and guided by the same statutory regime, the *United States v. Sofsky*[19] and *Zinn* courts formed vastly different conclusions with respect to the reasonableness of Internet-use bans as a term of supervised release.[20] This Note asserts that such inexplicable and arbitrary results regarding Internet-use bans are endemic under the existing, one-size-fits-all statutory guidance for supervised release terms. Because, under current law, judicial decisions to impose Internet-use bans are incoherent at best and arbitrary at worst, Congress should amend 18 U.S.C. § 3583(d)—the statute governing supervised release conditions—to provide judges with meaningful, cyber-specific guidance.

Part I of this Note provides a historical overview of child pornography laws and assesses the current state of the applicable regulations.

---

11 *Id.*

12 Brief and Appendix for the United States, *Sofsky*, 287 F.3d 122 (No. 01-1097), 2001 WL 36197385.

13 *Sofsky*, 287 F.3d at 124 (stating that Sofsky pled guilty to violating 18 U.S.C. § 2252A (a)2)(A) (2006)).

14 United States v. Zinn, 321 F.3d 1084 (11th Cir. 2003).

15 *Sofsky*, 287 F.3d at 124.

16 *Id.*

17 *Id.* at 126.

18 *Id.* (alteration in original) (quoting United States v. Peterson, 248 F.3d 79, 83 (2d Cir. 2001)) (internal quotation marks omitted).

19 United States v. Sofsky, 287 F.3d 122 (2d Cir. 2002).

20 *Compare* United States v. Zinn, 321 F.3d 1084, 1093 (11th Cir. 2003), *with Sofsky*, 287 F.3d at 126.

Additionally, it analyzes the United States Sentencing Guidelines for virtual child pornography cases and briefly describes the one-size-fits-all statutory regime governing supervised release conditions.

Part II explores the types of Internet-use restrictions most commonly imposed by the courts in virtual child pornography cases and examines the types of sources that guide the courts in determining the permissibility of such restrictions. Part II then discusses the alleged circuit split over the permissibility of Internet-use restrictions in child pornography cases. In discussing the so-called "split," this Part extracts broad themes and justifications from the cases affirming and rejecting Internet-use bans.

Part III outlines the Note's proposed statutory amendment, the **Un**dermining **I**nternet **F**elons' Ability to **O**btain **R**eadily Available Pornographic **M**aterials Act ("UNIFORM Act"), and applies this novel framework to the *Zinn* and *Sofsky* cases. The UNIFORM Act—meant to supplement, not replace, the existing statutory regime—would arm courts facing decisions regarding Internet-use bans with cyber-specific guidelines derived from the Sentencing Guidelines for child pornography offenses and the caselaw described in Part II.

Part IV summarizes and dispels four potential counterarguments to the UNIFORM Act. The first and second arguments contend that Internet-monitoring software and unannounced searches by POs provide a narrowly tailored alternative to full-scale Internet-use bans. The third counterargument asserts that the omnipresence of the Internet in modern society renders Internet-use bans unreasonable. The final counterargument concedes that Internet-use bans are permissible under certain factual circumstances, but disputes the UNIFORM Act's central hypothesis that decisions regarding such bans require individualized judicial guidelines.

At bottom, the Note posits a commonsense compromise that would promote consistency in an area currently plagued by judicial ambiguity.

I. Background on Virtual Child Pornography Statutes: Historical Evolution and the Current Landscape

A. Historical Regulation of Child Pornography

The term "child pornography" is generally understood to describe images of persons under the age of eighteen engaged in sexually explicit conduct.[21] Before the 1960s, no federal statute explicitly pro-

[21] Orin S. Kerr, Computer Crime Law 215 (2d ed. 2009).

hibited the receipt, distribution, and possession of these images.[22] Instead, child pornography images were regulated under obscenity law.[23] The contours and reach of federal and state obscenity laws at the time were generally dictated by the Supreme Court's First Amendment jurisprudence.[24] The Court originally held that the First Amendment did not protect obscenity,[25] thus enabling far-reaching obscenity laws. Ultimately, though, the Court in *Miller v. California*[26] narrowed the potential reach of state obscenity laws by proposing rigid guidelines for determining when an image was impermissibly obscene.[27]

States feared that *Miller* would render their obscenity laws either unconstitutional or ineffective.[28] They posited that *Miller*'s speech-protective mandate would enable widespread exploitation and abuse of minors.[29] Accordingly, many states, in an effort to avoid *Miller*'s reach, enacted laws specifically targeting child pornography.[30]

Responding to this wave of state legislation, the Court in *New York v. Ferber*[31] acknowledged that "the exploitive use of children in the production of pornography [had] become a serious national problem."[32] It further suggested that *Miller* granted First Amendment protection to many child pornography images.[33] The Court subsequently changed the nature of child pornography regulation forever, holding that "the [government is] entitled to greater leeway in the regulation of pornographic depictions of children."[34] This paved the way for comprehensive child pornography laws.[35]

---

22 *Id.*

23 *Id.*

24 *See id.*

25 Roth v. United States, 354 U.S. 476, 484–85 (1957). The Court defined obscene material as "material which deals with sex in a manner appealing to prurient interest." *Id.* at 487.

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

27 *Id.* at 24. Factors posited by the Court included (1) whether "the average person, applying contemporary community standards would find that the [image] . . . appeals to the prurient interest"; (2) whether the image "depicts or describes, in a patently offensive way, sexual conduct"; and (3) whether the image "lacks serious literary, artistic, political, or scientific value." *Id.* (internal quotation marks omitted).

28 *See* KERR, *supra* note 21, at 215.

29 *See id.*

30 New York v. Ferber, 458 U.S. 747, 749 n.2 (1982).

31 New York v. Ferber, 458 U.S. 747 (1982).

32 *Id.* at 749.

33 *See id.* at 753, 764–65.

34 *Id.* at 756. The Court unambiguously established that child pornography and obscenity are two separate categories of speech, neither of which is protected by the First Amendment. *See id.* at 764.

35 Before discussing the current federal landscape of child pornography regulation, it is instructive to examine the state laws that predated these statutes as they appear in their current

B. The Current Landscape: 18 U.S.C § 2252 and § 2252A

Congress began regulating the burgeoning child pornography market by enacting the Protection of Children Against Sexual Exploitation Act of 1977.[36] This is still the primary federal statute prohibiting child pornography distribution, receipt, and possession.[37] The statute, codified at 18 U.S.C. § 2252, contains four types of offenses.[38] The first prohibits knowingly transporting in interstate or foreign commerce a visual depiction of a minor engaging in sexually explicit conduct.[39] The second prohibits receiving or distributing such depictions.[40] The third and fourth prohibitions deal with possession-related crimes.[41] With respect to punishment, the statute draws a bright line at "mere possession." Child pornography crimes constituting (1) transporting or shipping, (2) receiving or distributing, or (3) selling or possessing with intent to sell trigger a five-year mandatory minimum prison sentence.[42] Mere possession crimes, on the other hand, do not trigger a mandatory minimum sentence.[43]

Legislators became increasingly concerned, however, that developing computer technologies were rendering § 2252 outdated.[44] Congress feared that new forms of pedophilia, enabled by these technologies, fell outside the reach of the statute.[45] It correspondingly

---

form. Before the Court's landmark decision in *Ferber*, twenty states prohibited the dissemination of material depicting children engaged in sexual conduct, regardless of whether the material was obscene. *Id.* at 749. The New York statute at issue in *Ferber*, for example, prohibited persons from knowingly promoting sexual performances by children under the age of sixteen by distributing material that depicts such performances. *Id.* at 750–51. Similarly, a Delaware law prohibited persons from knowingly receiving, distributing, or promoting child pornography. DEL. CODE ANN. tit. 11, §§ 1108–1109 (1979). As discussed below, these state statutes, which bear a striking resemblance to federal child pornography statutes in their present form, unmistakably laid the groundwork for comprehensive federal child pornography legislation.

36 Protection of Children Against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, sec. 2(a), § 2252, 92 Stat. 7, 7–8 (1978) (codified as amended at 18 U.S.C. § 2252 (2006)).

37 KERR, *supra* note 21, at 217.

38 18 U.S.C. § 2252; KERR, *supra* note 21, at 217.

39 18 U.S.C. § 2252(a)(1); KERR, *supra* note 21, at 217–18.

40 18 U.S.C. § 2252(a)(2); KERR, *supra* note 21, at 218.

41 18 U.S.C. § 2252(a)(3)–(4) (proscribing the sale of child pornography or the possession of such materials with the intent to sell, as well as the mere possession of such materials); KERR, *supra* note 21, at 218.

42 18 U.S.C. § 2252(b)(1); KERR, *supra* note 21, at 218.

43 18 U.S.C. § 2252(b)(2); KERR, *supra* note 21, at 218. They do, however, trigger a ten-year statutory maximum. 18 U.S.C. § 2252(b)(2).

44 KERR, *supra* note 21, at 218. Specifically, Congress was concerned about new computer software that allowed users to "morph" a digital image of a real child's face onto a computer-generated image of a child's body. *Id.*

45 *See id.*

enacted the Child Pornography Prevention Act of 1996,[46] followed by additional amendments in 2003,[47] to encompass these new forms of child pornography.

In substance, the amended child pornography statute, codified at 18 U.S.C. § 2252A, is merely an enhanced version of § 2252.[48] It does, however, directly address the heart of Congress's concerns at the time[49] regarding evolving computer technology. For example, Congress revised the definition of "child pornography" to include morphed images.[50] According to the new statute, child pornography includes "computer-generated image[s] that [are], or [*are*] *indistinguishable from*, that of a minor engaging in sexually explicit conduct; or . . . such visual depiction [that] has been created, adapted, or modified *to appear that* an identifiable minor is engaging in sexually explicit conduct."[51] By simply adding cyber-specific language to the definition of child pornography, Congress dramatically extended the reach of federal child pornography laws.[52]

---

46 Child Pornography Prevention Act of 1996, Pub. L. No. 104-208, § 121(2), 110 Stat. 3009-26, -27 (codified as amended at 18 U.S.C. § 2256) (definitions section); *id.* sec. 121(a), § 2252A, 110 Stat. at 3009-28 to -29 (codified as amended at 18 U.S.C. § 2252A). Rather than simply amending the existing law, Congress created an entirely new statute to supplement the Protection of Children Against Sexual Exploitation Act of 1977. KERR, *supra* note 21, at 218. It based this strategic decision on concerns that the new statute might be struck down on First Amendment grounds, leaving no child pornography law on the books. *Id.* Accordingly, under current law, the child pornography statute remains in force, with the amended child pornography statute operating independently. *Id.*

47 *See* PROTECT Act, Pub. L. No. 108-21, 117 Stat. 650 (2003) (codified in scattered sections of 18, 28, and 42 U.S.C.).

48 The new law affirms the prohibitions on transporting, shipping, receiving, and distributing child pornography. *See* 18 U.S.C. § 2252A(a)(1)–(4). Further, the statute mirrors the child pornography statute's possession-related offenses. *See id.* § 2252A(a)(5). Finally, the amended child pornography statute widens the scope of traditional child pornography laws by proscribing advertising and soliciting images of child pornography, and luring minors with such materials. *Id.* § 2252A(3)(B).

49 *See supra* notes 46–48 and accompanying text.

50 *See* 18 U.S.C. § 2256(8).

51 *Id.* (emphases added).

52 The Supreme Court, however, limited § 2252A's reach on constitutional grounds. *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). The Court held that, to the extent that the statute proscribed child pornography that did not depict actual children, it violated the First Amendment. *Id.* at 250 (determining that the exemption from First Amendment scrutiny announced in *Ferber* only applies to images of actual children, not purely virtual images). Under current law, therefore, the distinction between virtual and actual child pornography is paramount. *See, e.g.*, Lora v. Boland, No. 1:07 CV 2787, 2011 WL 5006055 (N.D. Ohio Oct. 20, 2011); United States v. Marchand, 308 F. Supp. 2d 498, 503–04 (D.N.J. 2004) (noting that the validity of a conviction under § 2252A turned on proving beyond a reasonable doubt that the image depicts a real child).

C. *United States Sentence Guidelines in Child Pornography Cases*[53]

Judges determine prison sentences for those who violate the child pornography statutes under the multi-factor United States Sentencing Guidelines.[54] Under current statutory law, the Guidelines play no formal role in a judge's decision regarding supervised release.[55] However, this Note ultimately contends that Congress should incorporate the Guidelines' inflexible framework into the existing supervised release regime.[56] A brief description of the Sentencing Guidelines is therefore appropriate.

Under the Guidelines, the sentencing judge follows a highly mechanical, six-step process.[57] First, the judge must select the set of offense guidelines that correspond to the defendant's crime.[58] This Note focuses exclusively on those provisions of the Guidelines that are tailored to child pornography cases. Second, the judge must determine the offense level for the crime.[59] Here, the judge assigns a base offense level.[60] All child pornography offenses, except for mere possession crimes, start at the same level.[61]

Third, the judge performs the crux of the sentencing analysis by assigning point values to specific offense characteristics.[62] The points are subsequently added to or subtracted from the base point level established in step two.[63] Offense characteristics trigger point increases when (1) the material involves a prepubescent minor or minor who had not attained the age of twelve, (2) the defendant distributes the pornographic material for pecuniary gain or to a minor with the intent of enticing the minor to engage in illegal nonsexual or sexual conduct, (3) the offense involves material that portrayed sadistic or masochistic conduct, (4) the defendant engages in a pattern of activity involving

---

53 For a comprehensive analysis of sentencing results in child pornography cases, see MARK MOTIVANS & TRACEY KYCKELHAHN, U.S. DEP'T OF JUSTICE, FEDERAL PROSECUTION OF CHILD SEX EXPLOITATION OFFENDERS, 2006 (2007), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/fpcseo06.pdf.

54 KERR, *supra* note 21, at 277.

55 *See* 18 U.S.C. § 3583 (establishing authorized terms, conditions, and factors to be considered in determining a term of supervised release without reference to the Guidelines).

56 *See infra* Part III.

57 This easily digestible framework is adopted from KERR, s*upra* note 21, at 278.

58 *Id.*

59 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2 (2010); KERR, *supra* note 21, at 278.

60 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(a); KERR, *supra* note 21, at 278.

61 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(a)(1)–(2); KERR, *supra* note 21, at 278.

62 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(b); KERR, *supra* note 21, at 278–79.

63 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(b); KERR, *supra* note 21, at 278–79.

the sexual abuse of a minor, or (5) the defendant utilizes a computer in committing the offense.[64] The judge, moreover, assigns offense points based on the number of pornographic images involved in the crime.[65]

Fourth, after assessing special offense characteristics, the sentencing judge applies upward and downward adjustments. The adjustments reflect the specific circumstances of the crime. For example, the judge may apply an upward adjustment for child pornography offenders who utilize a "special skill" in committing the crime.[66] Alternatively, the judge may apply a downward adjustment when the defendant accepts responsibility for the crime by pleading guilty.[67] Fifth, upon applying the upward and downward adjustments, the sentencing judge determines the defendant's criminal history category. A defendant receives offense points for all past criminal convictions.[68] If this is the defendant's first conviction, however, he receives no additional offense points.[69] Finally, the judge consults the Sentencing Guidelines table and assigns a sentencing range based on the defendant's offense level (determined at steps two through four) and criminal history category (determined at step five).[70] Overall, the Sentencing Guidelines significantly limit judicial discretion.

D. Supervised Release Guidelines in Child Pornography Cases

To understand the logic driving the UNIFORM Act, it is critical to juxtapose the rigid sentencing scheme outlined above[71] against the flexible statutory standards governing supervised release terms.[72] Where the Guidelines limit judicial discretion,[73] the statute governing supervised release terms enables unfettered judicial flexibility.

Under 18 U.S.C. § 3583(d), the court may impose a condition of supervised release to the extent that it (1) is reasonably related to the factors set forth in 18 U.S.C. § 3553(a) and (2) involves no greater

---

64 U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(b)(1)–(6).

65 *Id.* § 2G2.2(7).

66 *Id.* § 3B1.3.

67 *Id.* § 3E1.1.

68 *Id.* § 4A1.1; KERR, *supra* note 21, at 281.

69 U.S. SENTENCING GUIDELINES MANUAL § 4A1.1(x); KERR, *supra* note 21, at 281.

70 KERR, *supra* note 21, at 281–82.

71 *See supra* Part I.C.

72 More than half of all convicted sex offenders are placed on probation and assigned to POs. Krista L. Blaisdell, Note, *Protecting the Playgrounds of the Twenty-First Century: Analyzing Computer and Internet Restrictions for Internet Sex Offenders*, 43 VAL. U. L. REV. 1155, 1202 (2009).

73 *See supra* Part I.C.

deprivation of liberty than is reasonably necessary.[74] A sentencing judge thus employs a two-part test to determine the permissibility of the supervised release condition.

First, she determines whether the condition comports with § 3553(a).[75] This section instructs the judge to consider (1) the nature and circumstances of the offense and history and characteristics of the defendant, (2) whether the condition promotes respect for the law and provides just punishment, (3) whether the condition affords adequate deterrence to criminal conduct, (4) whether the term protects the public from further crimes of the defendant, and (5) whether the condition provides the defendant with needed education or other correctional treatment.[76]

Second, if the term is "reasonably related" to these broad statutory factors, the judge must determine whether it "involves no greater deprivation of liberty than is reasonably necessary."[77] Notably, the statute offers no meaningful guidance regarding what constitutes a substantial deprivation of liberty; that determination is left entirely to the sentencing judge.[78] The consequences of such unbridled discretion, illustrated below,[79] provide the driving force behind the UNIFORM Act.

II. Internet-Use Bans as a Condition of Supervised Release in Child Pornography Cases

Part II describes and compares the varying ways in which appellate courts have interpreted the permissibility of Internet-use bans in child pornography cases.

As background, certain district court judges derive from the supervised release guidelines the power to impose Internet-use bans on child pornography offenders.[80] The conditions themselves are relatively uniform across the federal courts.[81] The most common condition states that "the defendant shall not possess, procure, purchase or otherwise obtain access to any form of computer network, bulletin

74 18 U.S.C. § 3583(d)(1)–(2) (2006).

75 *Id.*

76 *Id.* § 3553(a).

77 *Id.* § 3583(d)(2).

78 *Id.*

79 *See infra* Part II.B–C.

80 *See, e.g.*, United States v. Thielemann, 575 F.3d 265, 270 (3d Cir. 2009); United States v. Zinn, 321 F.3d 1084, 1087 (11th Cir. 2003).

81 *Compare Thielemann*, 575 F.3d at 270, *with* United States v. Sullivan, 451 F.3d 884, 892 (D.C. Cir. 2006).

board, Internet, or exchange format involving computers [for the duration of his supervised release term] unless specifically approved by [his] U.S. Probation Officer."[82] The two most common characteristics are, therefore, (1) a blanket prohibition on Internet use and (2) an exception for Internet use upon obtaining the permission of a probation officer.[83]

A. Sources of Conflict

Before discussing the current state of the caselaw, it is instructive to consider the sources most often cited by courts considering the permissibility of Internet-use bans. These include (1) the statutory regime governing supervised release terms,[84] (2) the Constitution,[85] and (3) practical understandings of computer use in modern society.

With respect to the statutory regime, the courts examine the link between the Internet-use ban and the supervised release guidelines' twin statutory goals of deterring the offender from obtaining child pornography in the future and protecting the public.[86] As for the Constitution, the courts have noted the First Amendment implications of limiting an offender's Internet access.[87] With regard to practical

---

82 *See, e.g.*, United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001); United States v. Crandon, 173 F.3d 122, 127 (3d Cir. 1999).

83 *See Crandon*, 173 F.3d at 122. Although the courts do not explicitly outline the prior-permission process, it would likely constitute three steps. First, the parolee would submit a request to his PO with the URL he wishes to visit. Second, the PO would view the URL and either approve or deny the request. At this stage, the PO would likely use his discretion to determine whether allowing the parolee to visit the website would in any way endanger the public or facilitate recidivism. Third, to the extent that the request is approved, the PO would monitor the parolee to ensure that he indeed visited the URL for which he was approved. *See infra* Part IV.

It is worth noting, however, that at the margins, a few outlier courts have diverged from the standard condition. For example, one district court imposed an absolute lifetime ban on using computers and computer equipment, as well as accessing the Internet, with no exception for employment or education. *See* United States v. Voelker, 489 F.3d 139, 144 (3d Cir. 2007). However, such debilitating and permanent conditions are rare. This Note's solution specifically addresses the legitimate concern that future courts may impose such extreme conditions. *See infra* Part III.

84 *See* 18 U.S.C. § 3583(d) (2006).

85 U.S. CONST. amend. I.

86 *See* United States v. Rearden, 349 F.3d 608, 621 (9th Cir. 2003); United States v. Paul, 274 F.3d 155, 169–70 (5th Cir. 2001).

87 *Compare Voelker*, 489 F.3d at 150–53 (vacating a computer-use ban on First Amendment grounds), *with* United States v. Ritter, 118 F.3d 502, 504 (6th Cir. 1997) (upholding as valid a supervisory condition implicating freedom of speech as primarily designed to meet ends of rehabilitation and protection of the public). The issue of whether Internet-use bans violate the First Amendment falls outside the scope of this Note. However, for an interesting analysis of this rich topic, see Gabriel Gillett, Note, *A World Without Internet: A New Framework for Ana-*

considerations, the courts consider the indispensability of the Internet in modern society.[88]

The division among the courts of appeal[89] regarding the permissibility of Internet-use bans reflects the weight that each court allots to these three seemingly contradictory sources, as demonstrated below.[90]

B. Courts of Appeal Affirming the Permissibility of Internet-Use Bans

Zinn[91] is representative of the cases affirming Internet-use bans. Recall that Zinn pled guilty to possessing child pornography after U.S. Customs agents executed a search warrant for his home and recovered more than four-thousand child pornography images.[92] At sentencing, the court imposed the standard supervised release condition[93]: Zinn could not use the Internet without first obtaining permission from his PO.[94]

On appeal, Zinn argued that the supervised release condition was not reasonably related to the goals prescribed by the supervised release guidelines.[95] The Eleventh Circuit concluded, however, that the district court did not abuse its discretion in limiting Zinn's Internet use.[96] Although the court recognized that the Internet has become an important resource for information, communication, and commerce, it reasoned that the particular facts of this case highlighted the concomitant dangers of Internet use by child pornography offenders.[97] Accordingly, the Internet-use restriction was reasonably tethered to the statutory goals of protecting the public and the sex offender himself from recidivism.[98] The court further posited that because Zinn could

---

lyzing a Supervised Release Condition that Restricts Computer and Internet Access, 79 FORDHAM L. REV. 217 (2010).

88 *Voelker*, 489 F.3d at 148; United States v. Freeman, 316 F.3d 386, 392 (3d Cir. 2003).

89 *See infra* Part II.B–C.

90 *See* Emily Brant, Comment, *Sentencing "Cybersex Offenders": Individual Offenders Require Individualized Conditions when Courts Restrict Their Computer Use and Internet Access*, 58 CATH. U. L. REV. 779, 786 (2009). It is instructive, as this Note now turns to the purported circuit split over the permissibility of Internet-use bans, for the reader to keep in mind the relative weight each court assigns to these three policy considerations as a possible means to reconcile the seemingly contradictory results.

91 *See supra* notes 1–9 and accompanying text.

92 United States v. Zinn, 321 F.3d 1084, 1086 (11th Cir. 2003).

93 *See supra* text accompanying notes 80–83.

94 *Zinn*, 321 F.3d at 1087.

95 *Id.* at 1092.

96 *Id.* at 1093.

97 *Id.*

98 *Id.*

still use the Internet for valid purposes after obtaining his PO's permission, the condition did not constitute an undue deprivation of liberty.[99]

Zinn exemplifies the relative weight courts upholding Internet-use bans allot to each of the three sources outlined above.[100] These courts rely heavily on the supervised release guidelines' statutory goals.[101] In fact, nearly all cases affirming an Internet-use ban offer a blanket pronouncement, often without further explanation, that limiting the offender's Internet access is reasonably related to the important goals of deterring the offender from reverting to similar conduct and protecting the public.[102]

In holding that an Internet-use restriction is defensible as long as it is reasonably tethered to the supervised release guidelines' broad goals, the courts impliedly minimize the importance of the Internet. In fact, this consideration is typically either excluded from the courts' analyses entirely or mentioned in passing.[103] Accordingly, at the risk of oversimplifying the caselaw, the courts upholding Internet-use bans reason that ensuring deterrence and public safety outweighs competing concerns regarding the central role that the Internet plays in modern life.[104]

Two additional factors are sometimes cited in defense of blanket Internet-use restrictions. First, the courts reason that in cases where the child pornography offender utilized the Internet to entice or encourage real-time molestation of a child, restrictions on computer use are proportionate to the crime.[105] Second, appellate courts draw a key distinction between absolute bans on Internet use and conditional bans where the offender may access the Internet with his PO's permis-

---

99 *Id.*

100 *See supra* Part II.A.

101 *See, e.g.*, *Zinn*, 321 F.3d at 1093.

102 *See* United States v. Rearden, 349 F.3d 608, 621 (9th Cir. 2003); United States v. Paul, 274 F.3d 155, 170 (5th Cir. 2001); United States v. Crandon, 173 F.3d 122, 127–28 (3d Cir. 1999).

103 *See, e.g.*, United States v. Thielemann, 575 F.3d 265, 278 (3d Cir. 2009) (mentioned in passing); United States v. Sullivan, 451 F.3d 884, 895–96 (D.C. Cir. 2006) (not mentioned).

104 One court has defended such a balance from a defendant's perspective by stating, "If full access posed an unacceptable risk of recidivism, yet all controls on access were forbidden, then a judge would have little alternative but to increase the term of imprisonment in order to incapacitate the offender. Few defendants would deem that a beneficial exchange . . . ." United States v. Scott, 316 F.3d 733, 736–37 (7th Cir. 2003).

105 *See Thielemann*, 575 F.3d at 278; *Paul*, 274 F.3d at 169–70.

sion.[106] The latter conditions, according to these courts, do not constitute an unreasonable deprivation of the offender's liberty.[107]

C. *Courts of Appeal Rejecting the Permissibility of Internet-Use Bans*

Sofsky is often cited for its unequivocal rejection of Internet-use restrictions.[108] Recall that Sofsky pled guilty to receiving child pornography after the government presented overwhelming evidence that he received more than 1000 child pornography images on his home computer and exchanged the images over the Internet.[109] At sentencing, the district court imposed a prison term, followed by a three-year term of supervised release during which Sofsky was prohibited from "access[ing] a computer, the Internet, or bulletin board systems at any time, unless approved by the probation officer."[110]

The *Sofsky* court first remarked that "[c]omputers and Internet access [are] virtually indispensable in the modern world of communications and information gathering."[111] The court then offered a series of analogies to undermine the palatability of Internet-use bans.[112] It reasoned that although a defendant might use the telephone to commit fraud, this would not justify a condition of probation that includes an absolute ban on telephone use.[113] The same could be said, according to the court, of a prohibition on the use of the mail imposed on a defendant convicted of mail fraud.[114] The court thus held that the analogous supervised release condition in this case inflicted an unreasonable deprivation of the offender's liberty.[115]

More salient for our purposes, the court offered a second justification for its decision. It argued that broad Internet-use bans were unnecessary when more focused conditions, limited to blocking pornography websites, were available.[116] According to the *Sofsky* court, this narrower condition—enforced by unannounced inspections of the offender's home, undercover sting operations, or other monitoring

106 *See, e.g.*, United States v. Fields, 324 F.3d 1025, 1027 (8th Cir. 2003).

107 *See* United States v. Walser, 275 F.3d 981, 988 (10th Cir. 2001).

108 *See, e.g.*, United States v. Freeman, 316 F.3d 386, 391–92 (3d Cir. 2003).

109 *See* United States v. Sofsky, 287 F.3d 122, 124 (2d Cir. 2002).

110 *Id.* (internal quotation marks omitted).

111 *Id.* at 126 (first alteration in original) (quoting United States v. Peterson, 248 F.3d 79, 83 (2d Cir. 2001)) (internal quotation marks omitted).

112 *Id.*

113 *Id.* (citing *Peterson*, 248 F.3d at 83).

114 *Id.*

115 *Id.* at 127.

116 *Id.*

techniques—constituted an equally effective alternative to traditional Internet-use bans.[117] The court concluded that imposing the traditional Internet-use prohibition deprived the offender of his liberty rights in violation of the supervised release statute.[118]

As *Sofsky* illustrates, courts that are hostile toward Internet-use restrictions give significant weight to the practical importance of the Internet in modern life.[119] These courts posit that the Internet is a "vast repository" offering books, newspapers, and research tools.[120] A complete ban on Internet access consequently prevents benign use of e-mail and other commonplace computer uses, such as getting a weather forecast or reading an online newspaper.[121] Thus, the practical significance of the Internet, coupled with the availability of less restrictive alternatives to Internet-use bans, render the bans a greater deprivation of liberty than is reasonably necessary.[122]

Like the courts upholding Internet-use bans, however, those rejecting the condition do not rely entirely on the three sources listed at the outset of Part II. Rather, these courts consider three additional factors. First, the courts consistently invoke the mail and telephone analogies outlined in *Sofsky*.[123] Second, the courts offer two related factual circumstances under which Internet-use bans are per se unreasonable: (1) when the defendant did not use the Internet to solicit inappropriate contact with children, and (2) when the defendant did not have a past history of abusing digital communications.[124] Third, the courts consider the nature of the supervised release term itself. They consistently hold that lifetime Internet-use bans, as well as restrictions that do not provide for Internet access with a PO's permission, are overly broad.[125] The courts rejecting Internet-use restrictions, accordingly, draw a bright line between conditions that

---

117 *See id.*

118 *See id.* at 126.

119 *See id.*

120 United States v. Scott, 316 F.3d 733, 737 (7th Cir. 2003).

121 United States v. Freeman, 316 F.3d 386, 392 (3d Cir. 2003).

122 *See* United States v. Voelker, 489 F.3d 139, 146 (3d Cir. 2007); *Freeman*, 316 F.3d at 391–92; United States v. White, 244 F.3d 1199, 1206–07 (10th Cir. 2001).

123 *See Scott*, 316 F.3d at 737; *Sofsky*, 287 F.3d at 126. The *Scott* court took the analogy a step further in asserting that "[a] judge who would not forbid [a child pornography offender] to enter a video rental store (which may have an adult-video section) also should not forbid [her] to enter the Internet, even though Disney's web site coexists with others offering filthy pictures." *Scott*, 316 F.3d at 737.

124 *See Voelker*, 489 F.3d at 147–49; *Scott*, 316 F.3d at 737.

125 *See Voelker*, 489 F.3d at 147–49; United States v. Walser, 275 F.3d 981, 988 (10th Cir. 2001).

permit benign Internet access under PO supervision and those that do not.[126]

D. Areas of Agreement

In response to cases like *Zinn* and *Sofsky*, academics and judges alike have declared a circuit split over the per se permissibility of Internet-use bans.[127] A close examination of the caselaw addressing such bans, however, suggests otherwise. In fact, nearly all courts striking down Internet-use restrictions concede that sentencing judges may, under certain circumstances, impose *some* limitations on a child pornography offender's computer use.[128] This concession by courts striking down Internet-use bans sheds light on the areas in which courts unvaryingly agree. This Section explores three important areas of common ground.

First, nearly all courts conclude that extreme conditions, such as lifetime Internet bans that do not allow for computer use with PO approval, are overly punitive.[129] Therefore, to the extent that a child pornography offender's crime passes a certain threshold of severity[130] and the offender may view certain innocuous websites with his PO's permission,[131] many courts are willing to uphold an Internet-use ban.

Second, the courts overwhelmingly agree on the permissibility of Internet-use bans under one set of circumstances: when the defendant used the Internet to solicit inappropriate contact with children or has

---

126 Conditions that do not provide for some form of benign Internet access are essentially deemed per se impermissible. *See, e.g.*, *Voelker*, 489 F.3d at 147–49.

127 *See, e.g.*, Christopher Wiest, Note, *The Netsurfing Split: Restrictions Imposed on Internet and Computer Usage by Those Convicted of a Crime Involving a Computer*, 72 U. CIN. L. REV. 847, 850–61 (2003).

128 *Voelker*, 489 F.3d at 145–46; United States v. White, 244 F.3d 1199, 1206 (10th Cir. 2001). The courts only differ over when such a far-reaching restriction constitutes an impermissible "deprivation of liberty." *Compare* United States v. Freeman, 316 F.3d 386, 391–92 (3d Cir. 2003) (stating that a special condition forbidding the defendant from possessing any computer in his home or using any online computer service without the written approval of the probation officer involves a greater deprivation of liberty than is reasonably necessary to deter future criminal conduct), *with Walser*, 275 F.3d at 988 (stating that a total ban on Internet use is sufficiently narrow if it allows for computer access upon obtaining probation officer consent).

129 *See* United States v. Thielemann, 575 F.3d 265, 278 (3d Cir. 2009); *Voelker*, 489 F.3d at 145–46, 148. Indeed, no court affirming an Internet-use ban has approved such a severe condition. *See, e.g.*, United States v. Rearden, 349 F.3d 608, 621 (9th Cir. 2003); United States v. Fields, 324 F.3d 1025, 1027 (8th Cir. 2003).

130 The exact threshold varies from case to case. As discussed at length below, however, all courts seem to agree that Internet-use bans are necessary where the defendant used Internet child pornography to solicit illegal sexual contact with a minor. *See Voelker*, 489 F.3d at 146–47.

131 *See id.* at 147–48.

a history of doing so.[132] As one court put it, "Appellate courts have overturned conditions seen as overly restrictive, especially in cases involving simple possession of child pornography. In cases where defendants used computers . . . to commit crimes involving greater exploitation [of children], such restrictions [on Internet use] have been upheld."[133] Another court explicitly distinguished between defendants charged with mere possession of child pornography and those who use the Internet to solicit contact with children.[134] Indeed, this court seemingly announced a bright-line test to explain two inconsistent cases from its circuit: one in which the court overturned an Internet-use ban and another in which it affirmed a similar ban.[135] It noted that the case upholding the ban involved a defendant who used the Internet to contact and exploit victims, whereas the case overturning the restriction did not.[136] The court justified its decision in the former case by stating that the defendant's computer use was far more problematic and difficult to trace.[137] An Internet-use ban, according to the court, was the only viable option.[138]

Third, courts that affirm and courts that overturn Internet-use bans recognize the fundamental nature of the individual right at stake.[139] Specifically, even courts that uphold Internet-use restrictions concede that "computers and Internet access have become virtually indispensable in the modern world."[140] In this regard, the courts affirming Internet-use bans are indistinguishable from the courts striking them down. Indeed, these latter courts often justify their decisions by stressing that the Internet is "a vast repository, offering books, newspapers, magazines, and research tools."[141] All courts therefore appreciate the far-reaching consequences of Internet-use bans.[142]

---

132 *See, e.g.*, *id.* at 146–47; United States v. Crume, 422 F.3d 728, 733 (8th Cir. 2005).

133 *Fields*, 324 F.3d at 1027 (citations omitted).

134 *See Voelker*, 489 F.3d at 146–48.

135 *Id.* at 147–48.

136 *Id.*

137 *Id.*

138 *See id.* A number of other courts have similarly drawn a bright line with respect to defendants who use the Internet to solicit illegal contact with minors. *See* United States v. Crume, 422 F.3d 728, 733 (8th Cir. 2005); *Fields*, 324 F.3d at 1027; United States v. White, 244 F.3d 1199, 1205–06 (10th Cir. 2001).

139 *See, e.g.*, United States v. Zinn, 321 F.3d 1084, 1093 (11th Cir. 2003).

140 United States v. Peterson, 248 F.3d 79, 83 (2d Cir. 2001).

141 United States v. Scott, 316 F.3d 733, 737 (7th Cir. 2003).

142 *See, e.g.*, United States v. Thielemann, 575 F.3d 265, 278 (3d Cir. 2009); *Zinn*, 321 F.3d at 1093. The only difference between courts that affirm and courts that overturn these bans appears to be how much weight a given court assigns to the importance of the Internet compared to the supervised release statute's broad goals. *See supra* Part II.B–C.

These three areas of common ground between the courts suggest an underlying theory, which serves as the basis for the UNIFORM Act. In the area of virtual child pornography crimes, the current statutory framework grants unfettered leeway to judges in imposing Internet-use restrictions.[143] As a result, in the factually indistinguishable cases at the margins—such as those where courts are not presented with a lifetime ban or a defendant who used the Internet to initiate contact with a minor—some courts have upheld Internet-use bans and others have struck them down. These conflicting decisions are inconsistent at best and arbitrary at worse. They are not based on principled differences in statutory interpretation or even divergent policy goals. Although such inconsistency is perhaps acceptable when less fundamental liberties are at stake, decisions regarding individuals' Internet-use rights merit far more judicial uniformity.

III. The UNIFORM Act, Virtual Child Pornography–Specific Guidelines for Terms of Supervised Release

Part III sets forth the Note's solution to the conflicting results described above: the UNIFORM Act. The proposed law suggests child pornography–specific guidelines for determining the terms of supervised release. The new guidelines would be implemented as a statutory amendment parallel to the existing supervised release guidelines.[144] Unlike the existing guidelines, which provide broad statutory goals and leave their implementation to unbridled judicial discretion,[145] judges would apply the UNIFORM Act in much the same manner as the Sentencing Guidelines.[146]

Inspired by these Guidelines, the UNIFORM Act seeks to limit sentencing judges' discretion in child pornography cases. In contrast to the Guidelines,[147] however, the UNIFORM Act would not prescribe a suggested time frame for the supervised release term at the end of the analysis. Rather, it would offer three factual scenarios,

---

143 *See* 18 U.S.C. § 3583(d) (2006) (stating that a court may order "any other condition it considers to be appropriate" as a further condition of supervised release).

144 This is similar to the manner in which the amended child pornography statute was adopted by Congress to compliment the far broader child pornography statute. *Compare id.* § 2252A, *with id.* § 2252.

145 *See id.* § 3583(d).

146 In other words, the proposed amendment would present judges with a series of factors, some dispositive and others merely discretionary, to inform their ultimate decision regarding supervised release terms in child pornography cases.

147 *Cf.* U.S. Sentencing Guidelines Manual § 2G2.2 (2010).

based on the caselaw discussed in Part II, in which Internet-use bans were either mandatory or per se unreasonable. If these three scenarios do not apply to the case at hand, the Act would instruct the sentencing judge to consider a list of offense factors to guide her analysis. The UNIFORM Act is set forth in the table below.

Table. The UNIFORM Act

Threshold Factors (considered in the following order)	**Discretionary Factors** (only considered if threshold factors do not apply)
1. Sexual Acts with a Minor: A sentencing judge shall impose an Internet-use ban if the defendant used child pornography to entice or otherwise encourage a minor to engage in illegal sexual acts. **2. Previous Convictions:** A sentencing judge shall impose an Internet-use ban if the defendant was previously convicted of a child pornography–related crime under 18 U.S.C. § 2252A or 18 U.S.C. § 2252, no matter the nature of the crime. **3. Mere Possession**: A sentencing judge shall not impose an Internet-use ban if the defendant was convicted of mere possession of child pornography, absent extraordinary circumstances.	**1.** The material involved a prepubescent minor or minor who had not attained the age of twelve.[148] **2.** If defendant is charged with distribution, he did so for pecuniary gain. **3.** The offense involved material that portrays sadistic or masochistic conduct or other depictions of violence. **4.** The amount of images the offense involved.[149] **5.** The offender immediately accepted responsibility or otherwise cooperated with law enforcement officers.

A. Guidelines and Justifications

This Section explains the bases for the UNIFORM Act's threshold and discretionary factors, as well as the statutory limitations. Moreover, it suggests ways in which sentencing judges should apply the discretionary factors.

1. Threshold Factor One: Sexual Acts with a Minor

The first question posed to the sentencing judge by the UNIFORM Act is whether the offender used child pornography to entice or otherwise encourage a minor to engage in an illegal sexual act. If the answer is yes, the proposed guidelines instruct the sentencing judge to cut short the inquiry and automatically impose an Internet-

148 In 2006, ninety-five percent of those sentenced for violating a child pornography statute fell under this category. MOTIVANS & KYCKELHAHN, *supra* note 53, at 8 tbl.6.

149 In 2006, sixty-five percent of child pornography crimes for which the offender was convicted and sentenced involved more than ten images. *Id.*

use ban.[150] The first threshold factor is derived directly from the caselaw regarding Internet-use bans. Nearly *all* sentencing judges, no matter their ultimate position on the desirability of Internet-use bans, agree that offenders who use computers to solicit illegal sexual conduct with minors[151] would threaten the public if granted unfettered Internet access.[152] The first threshold factor, therefore, responds to this concern by requiring sentencing judges to limit the offender's Internet use under such circumstances.

2. Threshold Factor Two: Previous Convictions

If the first threshold factor does not apply, the UNIFORM Act orders the judge to consider whether the offender has previously been convicted of a child pornography–related crime or any crime involving the sexual exploitation of minors. If he has, the Act requires the sentencing judge to impose an Internet-use ban, regardless of the nature of the crime.[153]

The second threshold factor is derived from the caselaw, as well as the supervised release guidelines' statutory goals. Although the courts have not forged a uniform consensus in this area, even those courts that ultimately overturned Internet-use bans conceded that offenders who committed past offenses involving the sexual exploitation of children are particularly dangerous to the public.[154] These courts imply that offenders who have been punished for past crimes involving minors, yet committed another such crime, demonstrate a propensity for recidivism.[155] They therefore require additional monitoring.[156] Moreover, this practical intuition is consistent with the Sentencing Guidelines.[157] The Guidelines automatically impose increased prison time for repeat offenders.[158] The UNIFORM Act merely follows suit.

---

150 The length of the ban is discussed in Part III.A.5.

151 Examples of the types of behavior the courts have in mind include using computers to (1) seduce underage children or arrange sexual relations with such children, or (2) seek contact of any form with a minor. *See, e.g.*, United States v. Voelker, 489 F.3d 139, 146 (3d Cir. 2007).

152 *See supra* notes 132–39 and accompanying text.

153 Thus, a repeat offender could conceivably receive an Internet-use ban if he were charged in the instant case with mere possession of child pornography under, for example, 18 U.S.C. § 2252(a)(4) (2006).

154 *See Voelker*, 489 F.3d at 147.

155 *See id.*

156 *See id.*

157 See *supra* Part I.C. This is particularly relevant because this Note's proposal is modeled after these Guidelines.

158 *See supra* notes 68–70 and accompanying text.

3. Threshold Factor Three: Mere Possession

If the first and second threshold factors do not apply, the UNIFORM Act directs the sentencing judge to consider whether the offender is charged with a "mere possession" crime.[159] If the court is presented with such an offense, the Act prohibits it from ordering an Internet-use ban.[160] Many courts refuse to entertain a full-scale Internet ban when the offender is charged under the child pornography statutes' "mere possession" provisions.[161] Furthermore, the statutes themselves distinguish between mere possession and all other crimes when determining the defendant's level of culpability.[162] Therefore, absent extraordinary facts, such as an unconscionable number of child pornography images on the defendant's computer, the UNIFORM Act follows the courts and Congress's lead.

4. Discretionary Factors

If the three threshold factors do not apply, the UNIFORM Act sets forth offense characteristics[163] for judges to consider when determining the permissibility of an Internet-use restriction. Consistent with the existing supervised release guidelines' goal of judicial flexibility,[164] these discretionary factors merely provide the sentencing judge with possible justifications for his or her decision. Keeping the goal of uniformity in mind, however, the UNIFORM Act predicts that if all judges begin their inquiry from the same analytical footing, uniform sentencing decisions in factually analogous cases will follow. At the very least, one would expect that judges provided with concrete sentencing factors would offer more robust justifications for their decisions concerning Internet-use rights.

No single factor would be dispositive. Nonetheless, the presence of factors one through three would seem to justify imposing an Internet-use ban. These three factual scenarios from the Sentencing

159 *See supra* Part I.B–C. In other words, the court must determine whether the evidence indicates that the offender downloaded illegal images, but did not attempt to sell or distribute them. *But see supra* text accompanying note 156. Remember, the third threshold factor only applies if this is the offender's first child pornography–related crime.

160 *See supra* Part III.A.

161 *See, e.g.*, *Voelker*, 489 F.3d at 143, 145–49; United States v. Crume, 422 F.3d 728, 730, 733 (8th Cir. 2005). *But see* United States v. Zinn, 321 F.3d 1084, 1086, 1093 (11th Cir. 2003); United States v. Walser, 275 F.3d 981, 985, 988 (10th Cir. 2001).

162 Recall, with regard to sentencing, these statutes impose a mandatory minimum for all child pornography crimes except mere possession. *See supra* Part I.B–C.

163 These offense characteristics were deemed relevant to sentencing decisions by the Federal Sentencing Guidelines. *See supra* Part I.C.

164 *See supra* Part I.D.

Guidelines[165]—offenses involving images of a prepubescent minor, distributing child pornography for pecuniary gain, and offenses involving images portraying particularly violent behavior—constitute the most reprehensible forms of child pornography violations. An Internet-use ban is necessary under such circumstances to (1) deter like-minded individuals from committing these especially heinous crimes and (2) deny those who have demonstrated a propensity for committing such offenses the technological capabilities to do so again.

The fourth factor, the number of child pornography images that the crime involved, could cut either way. Judges would treat this factor as a sliding scale: as the number of images increases, the permissibility of an Internet-use ban would increase proportionally. The same justification proffered directly above validates the sliding scale approach. To the extent that child pornography crimes involving a large number of images are more socially deplorable,[166] an Internet-use ban is necessary to deter similar conduct and deny those predisposed to committing child pornography crimes[167] the technological means to repeat their offense.[168]

Finally, any offender who cooperated with law enforcement officers, as described in the fifth factor, would strengthen his argument against an Internet-use ban. This factor is justified on three grounds. First, it promotes personal responsibility. Second, it preserves judicial and prosecutorial resources.[169] Third, because this factor promotes cooperation with police, it would fundamentally undermine the robust child pornography industry. An example illustrates this point. If an offender is charged with receiving and possessing child pornography

---

165 *See supra* notes 62–65 and accompanying text.

166 This seems to be an uncontroversial proposition. Child pornography crimes involving many images are more likely to exploit more children, either as the subjects of the images themselves or as targets of offenders who seek to use the images to entice child victims for illegal sexual contact. *See supra* Part I.A.

167 This Note assumes that those convicted of child pornography crimes are predisposed to committing such crimes.

168 Although the tipping point at which the number of images becomes particularly problematic would be left to each judge's discretion, it would seem that any offense involving more than 100 images would merit close consideration with respect to whether an Internet-use ban is appropriate. *Cf.* United States v. Zinn, 321 F.3d 1084, 1086 (11th Cir. 2003) (4000 images). On the other hand, any crime involving fewer than 10 images would almost certainly render an Internet-use ban inappropriate. *Cf.* U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(7) (2010) (imposing no offense-level increase for fewer than 10 images). Not only is a crime involving fewer than 10 images less troublesome on its face, it is possible, with so few images at issue, that the offender is merely exploring or downloaded the images accidentally.

169 Prosecutors and judges could focus their attention on other cases if child pornography offenders pled out earlier in the process.

and decides to cooperate with law enforcement, he would likely share information about his child pornography source.[170] The police could, in turn, use this information to investigate and arrest the distributor. Then, if the distributor similarly cooperated with police, a domino effect would ensue.

To reiterate, judges would likely not consider every discretionary factor in every case. Further, they would not necessarily assign the same weight to each of the discretionary factors. Such detailed guidance would, however, naturally lead to more uniform, or at the very least more defensible, results.

5. Statutory Limitations

Finally, The UNIFORM Act imposes two binding limits on sentencing judges' decisions regarding Internet-use bans. First, Internet-use restrictions must provide an exception for benign Internet use upon obtaining PO permission. This was a point of agreement among all courts,[171] particularly in light of the increasing importance of the Internet in modern society.[172]

Second, the Act would impose a three-year maximum limit on Internet-use bans. Although arbitrary at first glance, this limit appropriately balances the gravity of the offense with the right at stake. On the one hand, three years is long enough to deter child pornography offenses and deny convicted child pornography offenders the means to commit similar crimes in the short term. On the other hand, three years is short enough that offenders will reclaim their Internet-use rights in time to avoid long-term harm with respect to employment prospects[173] and informational access.[174]

B. Revisiting Zinn *and* Sofsky

The UNIFORM Act seeks to ensure more consistent results[175] with regard to Internet-use bans as a term of supervised release. It is therefore imperative to test the conclusion that the Act's rigid guidelines would achieve such uniformity. To do so, this Note revisits the

---

170 The source would likely be a website, but could conceivably be a friend or colleague.

171 *See supra* Part II.D.

172 *See, e.g.*, United States v. Voelker, 489 F.3d 139, 148 (3d Cir. 2007).

173 Under the UNIFORM Act, offenders could maintain jobs that require them to use computers during the supervised release period as long as they receive prior permission from their PO. *See supra* Part III.A.

174 Similarly, under the Act, offenders could access news and entertainment sources as long as they obtain PO permission.

175 *See supra* Part III.A.

Zinn and *Sofsky* cases.[176] These were cases in which the courts came to different conclusions regarding the permissibility of Internet-use bans despite near-identical factual circumstances.[177] This Note proffered these two cases in particular to illustrate the contradictory sentencing results that plague the existing statutory regime.

Zinn, as you might recall, ordered child pornography videos from a website operated by the U.S. Customs Service as part of an undercover operation.[178] He ultimately pled guilty to violating the amended child pornography statute.[179] Sofsky, on the other hand, stored numerous child pornography images on his computer and traded some of them across the Internet, although he never obtained a profit for these exchanges.[180] He ultimately pled guilty to receiving child pornography.[181] The sentencing judges in each case imposed an Internet-use ban as a term of supervised release.[182] On appeal, however, the *Sofsky* court overturned the supervised release term,[183] whereas the *Zinn* court deemed it permissible under the circumstances.[184] This Note now applies the UNIFORM Act to these cases to test if the Act would engender a different result.

First, applying the UNIFORM Act to *Zinn*, the sentencing judge would conclude that the offender did not use the Internet to entice a minor to engage in illegal sexual acts, nor was he previously convicted of a child pornography–related crime. The first and second threshold factors therefore do not apply.[185] However, because he was charged with mere possession of child pornography, the third threshold factor would prohibit the sentencing judge from imposing an Internet-use ban.[186]

Next, the sentencing judge would apply the UNIFORM Act to *Sofsky*. In this case, the offender similarly did not use the Internet to solicit sex from a minor.[187] Moreover, he was not previously convicted of a child pornography–related crime.[188] Unlike Zinn, though, Sofsky

176 *See supra* Part II.C–D.
177 *See supra* Part II.C–D.
178 *See* United States v. Zinn, 321 F.3d 1084, 1086 (11th Cir. 2003).
179 *Id.*
180 *See* United States v. Sofsky, 287 F.3d 122, 124 (2d Cir. 2002).
181 *Id.*
182 *See Zinn*, 321 F.3d at 1087; *Sofsky*, 287 F.3d at 124.
183 *Sofsky*, 287 F.3d at 126–27.
184 *Zinn*, 321 F.3d at 1093.
185 *See supra* Part III.A and text accompanying notes 150–59.
186 *See supra* Part III.A and text accompanying notes 159–63.
187 *Sofsky*, 287 F.3d at 124–25.
188 *Id.*

was charged with receiving child pornography, not mere possession.[189] The third threshold factor, consequently, would not apply.[190] The sentencing judge, at this point, would revert to the UNIFORM Act's discretionary factors. Here, although Sofsky's crime involved a large number of images,[191] which supports imposing an Internet-use ban, none of the other discretionary factors cuts in favor of such a ban. For instance, Sofsky ultimately pled guilty.[192] Further, there is no evidence that Sofsky's images depicted a prepubescent minor or that he exchanged the images for pecuniary gain.[193] Only one of the Act's discretionary factors justifies imposing a ban. Under such factual circumstances, it seems likely that a sentencing judge applying the UNIFORM Act would reach the same conclusion as a judge applying the Act to the facts in *Zinn*: an Internet-use ban is impermissible.

IV. Possible Counterarguments Against Changing the Existing Statutory Regime

The UNIFORM Act provides rigid child pornography–specific guidelines for judges determining whether to impose an Internet-use ban in such cases.[194] This Part addresses four potential counterarguments to this proposal.

A. The Sofsky *Alternatives*

Many of the courts of appeal that overturn Internet-use prohibitions assert that unannounced searches by POs and Internet-use monitoring provide sustainable alternatives to full-scale bans.[195] These two counterarguments are rooted in the *Sofsky* case, in which the court asserted that "a more focused restriction, limited to pornography sites and images," could be enforced by a combination of physical and electronic monitoring.[196]

---

189 *Id.* at 124.

190 *See supra* Part III.A.

191 Sofsky was convicted of possessing more than 1000 images of child pornography. *Sofsky*, 287 F.3d at 124. This is above the "tipping point" that this Note suggested might merit close consideration of imposing an Internet-use ban. *See supra* note 168.

192 *Sofsky*, 287 F.3d at 124.

193 *Id.*

194 *See supra* Part III.A–B.

195 *See Sofsky*, 287 F.3d at 126–27.

196 *See id.* at 127.

1. Physical Monitoring

Some consider physical monitoring—such as unannounced inspections of offenders' home computers by POs or government-led sting operations—as constituting a less intrusive and equally effective alternative.[197] This alternative, in theory, would ensure that the offender does not visit certain court-proscribed websites. But this argument defies practical understandings of PO resources and capabilities. To the extent that POs have sufficient time to physically monitor the thousands of child pornography offenders in this country,[198] they lack the funding, technical training, and equipment required to execute the monitoring envisioned by *Sofsky*.[199]

Even assuming for a moment that departments dedicated sufficient funds to adequately train POs, the child pornography offenders would likely remain savvier than the officers monitoring them.[200] They could easily devise ways to escape physical detection by disguising forbidden Internet use.[201] For example, offenders subject only to physical monitoring could easily procure low-cost software that enables them to wipe their hard drives clean of improper browsing history.[202] Further, to the extent that physical monitoring schemes would likely focus on the offender's home and work computers, the offender could access the Internet unchecked at a friend's house or local Internet café.[203] This purportedly less restrictive means of preventing

---

197 *See, e.g.*, *id.*

198 In 2006, 1209 individuals were convicted of committing a child pornography–related crime, MOTIVANS & KYCKELHAHN, *supra* note 53, at 6 tbl.7, and 2376 were charged, *id.* at 2 tbl.2.

199 *See* Art Bowker & Michael Gray, *An Introduction to the Supervision of the Cybersex Offender*, 68 FED. PROBATION, Dec. 2004, at 3, 7; Brant, *supra* note 90, at 805.

200 *See* Brant, *supra* note 90, at 805.

201 *See id*.

202 *See, e.g.*, United States v. White, 244 F.3d 1199, 1206–07 (10th Cir. 2001); Brant, *supra* note 90, at 804–05.

203 *See* Brant, *supra* note 90, at 804–05. One might assert that this easy means by which a parolee could circumvent physical detection of content-based violations would also undermine this Note's proposed UNIFORM Act. In other words, to the extent that the UNIFORM Act envisions circumstances under which full-scale Internet-use bans would be justified, the parolee could impermissibly use the Internet on a friend's home computer without detection, for example, in the same way that he could circumvent physical supervision by using his friend's machine. However, the ease with which POs could prove violations of an Internet-use ban, as opposed to a content-specific restriction, would likely deter parolees from attempting the circumvention strategy discussed here. After all, to prove a violation of an Internet-use ban, the PO would merely need to show that the parolee logged on to a computer. He could easily meet this burden by interviewing the parolee's friend or viewing the Internet café's video surveillance. To prove a violation of a content-specific restriction, on the other hand, the PO, already limited by drastic shortages in time and resources, would need to examine the friend's or Internet café's URL logs and demonstrate that the parolee, and not another user, accessed the impermissible websites.

recidivism consequently overestimates PO monitoring capabilities and underestimates simple ways offenders could avoid physical detection.[204]

2. Electronic Monitoring

Others contend that electronic monitoring—such as high-tech filtering devices to ensure compliance with specific website restrictions[205]—provides a less invasive option. The software endorsed by these advocates is installed directly onto the offender's computer and programmed to interpose a barrier between the computer's web browser and Internet connection.[206] Once installed, the software filters objectionable material either by blacklisting or whitelisting certain websites.[207] The former technique denies access to all websites placed on the computer's blacklist.[208] The latter technique blocks access to all sites *not* included on the so-called "whitelist" of permissible URLs.[209]

Several appellate courts confronting the permissibility of Internet-use restrictions have adopted this counterargument.[210] Electronic monitoring devices do not deprive the offender of his liberty in the same way that Internet-use bans do because, according to these courts, the devices permit innocuous Internet use, such as accessing e-mail or obtaining weather forecasts.[211] These courts asserted that the electronic software strikes the proper balance between preventing re-

---

Knowing the difficulties that the PO would encounter in proving a violation of a content-specific restriction as opposed to an Internet-use ban, the parolee would be far more tempted to breach his terms of supervised release.

204 *See id.*

205 *See White*, 244 F.3d at 1206; Thomas B. Nachbar, *Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character*, 85 MINN. L. REV. 215, 224 (2000).

206 *See White*, 244 F.3d at 1206; Nachbar, *supra* note 205, at 224.

207 *See White*, 244 F.3d at 1206; Nachbar, *supra* note 205, at 224.

208 *White*, 244 F.3d at 1206; Nachbar, *supra* note 205, at 224.

209 *See White*, 244 F.3d at 1206; Nachbar, *supra* note 205, at 224. Internet-content filtering is accomplished by using software to compare information about content with a set of filtering criteria before displaying the content on the user's computer monitor. Nachbar, *supra* note 205, at 223. This technology is known as "filtering" because the browser lets only certain content through the filter to the computer user. *See id.* The filtering software was originally designed to restrict children from accessing pornography, hate groups, and other material that parents wished to prevent them from using. *White*, 244 F.3d at 1206 n.8.

210 *See* United States v. Freeman, 316 F.3d 386, 392 (3d Cir. 2003); *White*, 244 F.3d at 1206.

211 *See Freeman*, 316 F.3d at 392.

cidivism and protecting the public and preserving the offender's liberty.[212]

Electronic monitoring may *one day* present a less intrusive and equally effective alternative to Internet-use bans as the courts above suggest. The evidence below, however, indicates that this fledgling technology is flawed for four reasons. The technology is thus unfit at the present time to replace broad computer-use bans.

First, the filtering devices only regulate content on the computer in which they are installed.[213] Accordingly, an offender can easily circumvent court-imposed whitelists or blacklists by logging on to a friend's computer, for example.[214] The friend's computer, obviously, would not contain the necessary filtering technology. If courts relied on physical monitoring to prevent offenders from using the friend's machine, POs could not practically prevent such activity for the reasons mentioned above.[215]

Second, software is presently available to erase from a computer's hard drive the names of websites visited.[216] Any child pornography offender with sufficient funds to afford this relatively inexpensive software could visit proscribed websites without detection.[217]

Third, given the rapid proliferation of Internet communication and creation of thousands of new websites every day, the software envisioned by the courts depends on continual updating.[218] Maintaining and updating this complex technology thus requires significant technical expertise and funding, which most local police departments do not possess.[219]

Fourth, if the court imposes a blacklist program,[220] it is impossible, given the ever-expanding scope of the Internet, to ensure that the software continues to prevent the offender from trafficking child por-

---

212 *See* United States v. Holm, 326 F.3d 872, 879 (7th Cir. 2003); Brant, *supra* note 90, at 803.

213 *White*, 244 F.3d at 1206.

214 Brant, *supra* note 90, at 805; *see also supra* notes 197–203 and accompanying text (addressing the same factual scenario in the context of physical monitoring as it relates to this Note's proposed UNIFORM Act).

215 *See supra* Part IV.A.1.

216 *See White*, 244 F.3d at 1206.

217 *See id.* at 1206–07.

218 *Id.* at 1206.

219 *See* Bowker & Gray, *supra* note 199, at 7–8 (describing the extensive training that officers should undergo to effectively supervise sex offenders); Brant, *supra* note 90, at 805 (noting that POs often lack that training or the funding to get it).

220 *See supra* note 208 and accompanying text.

nography.[221] An example illustrates this shortcoming. Suppose that a jury convicts a defendant[222] of selling child pornography over the Internet in violation of the child pornography statute.[223] The district court judge, believing that blanket Internet-use bans deprive the defendant of his liberty, enlists a PO to install an electronic filtering device on the defendant's computer.[224] The PO installs the device on July 4, 2011, and programs it to blacklist any website containing images of nude children or adults.[225] Now suppose that on July 5, 2011, a website is created that contains thousands of child pornography videos. The existing filtering device would not recognize this website because it was not included on the July 4 blacklist. Thus, the defendant could view this website without detection until the software was updated to include this website or a PO sifted through Defendant's browsing history.[226]

Although electronic monitoring may one day constitute a practical alternative to blanket Internet-use bans,[227] the current ease with which offenders could circumvent such devices poses too great a risk. Widespread reliance on this novel technology is premature.

B. The Power of the Internet Trumps All

Still others contend that, although Internet-use bans were reasonable in an era when commerce, employment, and recreation did not rely entirely on the Internet, such restrictions are unreasonable today. In other words, the fundamental right to access the Internet[228] outweighs any possible policy justifications for imposing a complete In-

---

221 *See White*, 244 F.3d at 1206. This shortcoming, admittedly, does not apply to whitelisting technology. Recall, whitelisting software only allows a computer user to access certain approved websites. *Id.* The user cannot access any other sites, whether they were accessible the day the software was installed or were created at some later date. *See supra* note 209 and accompanying text. The effectiveness of this technology, therefore, is unhindered by the creation of new, objectionable websites. However, this fact is not necessarily fatal to the Note's proposition that electronic monitoring does not yet serve as an adequate alternative to Internet-use bans. Indeed, the three other shortcomings noted above apply equally to whitelisting and blacklisting technology.

222 This hypothetical is not intended to reflect the facts of any particular case. Any resemblance it may bear to a specific case is entirely unintentional.

223 18 U.S.C. § 2252(a)(2) (2006).

224 *See, e.g.*, *White*, 244 F.3d at 1206–07.

225 *See id.*

226 This is true unless, of course, the defendant obtained software to delete the browsing history from his hard drive. If he did, the physical inspection would not uncover that he visited a banned website. *See supra* note 202 and accompanying text.

227 This Note concedes that such blanket bans are a far blunter tool.

228 *See, e.g.*, United States v. Scott, 316 F.3d 733, 736–37 (7th Cir. 2003).

ternet-use ban. These proponents, however, ignore the most powerful policy justifications for the more intrusive condition.

First, the supervised release statute itself identifies the most common defense of Internet-use bans in child pornography cases: deterring future criminal conduct.[229] With respect to deterrence, the courts reason that, insofar as the offender demonstrated a propensity for using the Internet to commit child pornography–related crimes, Internet-use bans effectively deter future, similar conduct.[230] The very intrusiveness fueling the counterargument that the condition is unreasonable in modern society is the only thing that ensures its strong deterrent effect.[231]

The unique threat that child pornography offenders potentially pose to the public constitutes the second, and most powerful, policy justification for limiting an offender's Internet-use rights.[232] In cases where child pornography offenders use such material to encourage other children to engage in illegal sexual acts,[233] restricting the offender's Internet access protects other children from similar exploitation.[234] The far-reaching scope of the Internet prohibition cited by opponents of such restrictions ensures its effectiveness in protecting unsuspecting child victims.[235]

Although most courts stop at the two policy justifications discussed above, two more nuanced policy arguments strongly justify computer-use bans. The first is derived from the statutory guidelines. It posits that preventing a child pornography offender from utilizing the Internet serves an important rehabilitative function.[236] The courts upholding Internet-use bans do not typically cite this statutory justification.[237] Nevertheless, Internet-use bans serve two rehabilitative functions. First, they rehabilitate the offender by blocking his strong temptation to view illicit materials. Second, they afford the offender time to reflect upon his past conduct and reach out for clinical support if necessary.

---

229 *See* 18 U.S.C. § 3553(2)(B)–(C) (2006).

230 *See* United States v. Thielemann, 575 F.3d 265, 278 (3d Cir. 2009); United States v. Paul, 274 F.3d 155, 169 (5th Cir. 2001).

231 *See, e.g.*, *Paul*, 274 F.3d at 170.

232 *See id.* at 169.

233 *See, e.g.*, *id.*

234 *See id.*

235 *See id.*

236 *See* 18 U.S.C. § 3553(2)(D) (2006).

237 *See supra* Part II.B.

The second and more nuanced policy justification emanates from the Seventh Circuit's opinions on this topic. The Seventh Circuit defends Internet-use bans from the offender's perspective, offering the most practical justification for Internet-use bans.[238] According to the court, "[i]f full [Internet] access posed an unacceptable risk of recidivism, yet all controls on access were forbidden, then a judge would have little alternative but to increase the term of imprisonment in order to incapacitate the offender. Few defendants would deem that a beneficial exchange . . . ."[239] The court's argument presupposes two conclusions endorsed in Part IV.A, addressing counterarguments one and two: (1) electronic and physical monitoring do not constitute an equal alternative to Internet-use bans, and (2) affording full Internet access to child pornography offenders upon their release from prison poses a risk of recidivism.[240] However, if one accepts these two propositions, the Seventh Circuit asserts that far-reaching Internet-use bans are more desirable to the criminal defendant than the alternative: "the more regimented life in prison."[241]

The four policy justifications for imposing Internet-use restrictions discussed above—deterrence, public safety, rehabilitation, and offenders' freedom—plainly outweigh the offenders' right to utilize a computer.

C. Judicial Discretion Trumps Broad Congressional Mandates

Those subscribing to this final argument claim that the existing supervised release guidelines properly leave fact-intensive decisions regarding supervised release to judicial discretion. They are hostile toward rigid judicial constraints imposed by Congress. In response, this Section asserts that the glaringly inconsistent results concerning Internet-use bans under the existing discretionary regime[242] are intolerable when the right to utilize the Internet is at stake[243] and that rigid congressional guidelines are a superior alternative.

One may justifiably ask what makes the specific term of supervised release discussed here—Internet-use bans—entitled to individu-

---

238 *See* United States v. Scott, 316 F.3d 733, 736–37 (7th Cir. 2003).

239 *Id.*

240 *See id.*

241 *Id.* at 737.

242 *See supra* Part II.B–C.

243 For a thorough examination of the increased role of the Internet in modern society, see Jake Adkins, Note, *Unfriended Felons: Reevaluating the Internet's Role For the Purpose of Special Conditions in Sentencing in a Post-Facebook World*, 9 J. ON TELECOMM. & HIGH TECH. L. 263, 271–74 (2011).

alized guidelines. The answer lies in the very right at stake in the sentencing decisions at issue, unimpeded Internet access. As illustrated in Part II.D, "computers and Internet access have become virtually indispensable in the modern world."[244] They offer users unparalleled access to entertainment and education-related resources, including "books, newspapers, magazines, and research tools."[245] The Internet further constitutes the means by which many modern businesses transact with consumers.[246] With the increasingly fundamental right to use the Internet at stake,[247] overly broad policy guidance, such as promoting public safety and preventing recidivism,[248] is insufficient. Instead, individualized guidelines that ensure predictable results, like those proposed in the UNIFORM Act, are necessary.

CONCLUSION

The UNIFORM Act seeks to reconcile three interests: (1) preserving judicial discretion in decisions regarding supervised release, as prescribed by the existing supervised release statute, (2) protecting the public from certain child pornography offenders, and (3) promoting judicial uniformity and predictability with respect to offenders' fundamental right to access the Internet. Because the existing regime's overwhelming preference for the first interest produces inconsistent decisions, often without explanation, the UNIFORM Act seeks to strike a more appropriate balance.

244 United States v. Peterson, 248 F.3d 79, 83 (2d Cir. 2001).

245 *See Scott*, 316 F.3d at 737.

246 *See id.*

247 This is a right with implications in nearly every facet of the offender's professional and private lives. *See id.*

248 18 U.S.C. § 3553(a) (2006).