ACCESS DENIED: Imposing Statutory Penalties on Sex Offenders Who Violate Restricted Internet Access as a Condition of Probation

Jane Adele Regina[†]

[†] J.D. candidate, 2008, Seton Hall University School of Law; B.A. Honors, Professional Writing, 1996, The College of New Jersey. I thank Professor Frank Pasquale for his tremendous insight and encouragement during the development of this comment. My deepest gratitude also extends to my family, particularly my mother, Rosemary, for her incredible support.

I. INTRODUCTION

Personal computers, according to Bill Gates, "have become the most empowering tool we've ever created. They're tools of communication . . . of creativity . . . and they can be shaped by their user."[1] In particular, the changing breadth of intellectual property law reflects the popularity of the Internet and its influence on the American legal landscape. Current statistics indicate that over 69% of the population of the United States uses the Internet.[2] This represents an explosion of online computer activity in society. Innovation invites the potential for abuse, however, and pornography occupies a significant sector of the Internet marketplace.[3] While it is almost impossible to inventory the wealth of available online data, the prevalence of online pornography reportedly accounts for 12% of all Internet websites, 25% of total search engine requests, and 35% of all monthly peer-to-peer downloads.[4] Within these, approximately 100,000 websites offer illegal child pornography.[5]

Courts are quick to convict traffickers who market in online pornographic material involving children, but disagree as to the appropriate degree of punishment when an offender is released on probation subject to special conditions imposed at sentencing.[6] Specifically, the courts of appeals are divided over sentencing sex offenders convicted of offenses relating to child pornography.[7] Some courts impose limitations on computer use or Internet access restricted as

---

[1] William Henry Gates III, General Partner, Microsoft Corp., Address at the University of Illinois Urbana-Champaign (Feb. 24, 2004).

[2] Nielsen/NetRatings dated December 31, 2007 indicate the U.S. Census Bureau estimates the population of the United States at almost 302 million people, and more than 215 million people reportedly use the Internet. Internet World Stats, http://www.internetworldstats.com/stats14.htm (last visited Dec. 31, 2007).

[3] *See* Jerry Ropelato, *Internet Pornography Statistics*, TopTenReviews.com, http://internet-filter review.toptenreviews.com/internet-pornography-statistics.html.

[4] *Id.* The term "peer-to-peer" refers to a network of people who are logged onto a computer system to share and deliver specified files between them, unlike a client/server configuration where users download resources from one main computer server.

[5] *Id.*

[6] *Compare* United States v. Paul, 274 F.3d 155 (5th Cir. 2001), *cert. denied*, 122 S. Ct. 1571 (2002) (rejecting the defendant's argument that the Internet was an indispensable tool in modern society, to impose a blanket prohibition against Internet access), *with* United States v. White, 244 F.3d 1199 (10th Cir. 2001) (remanding to revise the probationary condition as overly broad because it denied the defendant from using a computer for research purposes).

[7] *See, e.g.*, *supra* note 6.

a condition of probation while others forbid defendants from any form of online access.[8] Cases throughout the circuits have held both for and against the restriction, permitting Internet access in some cases only after probationers seek permission from probation officers.[9] Those circuits that choose to impose a ban on Internet access enforce the condition by employing a variety of methods to monitor defendants, including unannounced inspections of an offender's hard drive, installation of monitoring and filtering technology on the offender's computer, and initiated invitations of pornographic Internet material to offenders.[10]

The Supreme Court justified the use of reasonable conditions that deprive probationers of some freedoms by acknowledging that probationer status removes the "absolute liberty to which every citizen is entitled."[11] While this existing jurisprudence indicates a willingness to limit the First and Eighth Amendment rights of parolees,[12] the Supreme Court has not resolved Fourth Amendment issues implicated by subsequent monitoring of a convicted defendant's computer activity. Consequently, the Internet restriction debate centers on whether it is both constitutional and practical to enforce a total ban on Internet access.[13] In those courts that do allow offenders restricted access as a condition of probation or supervised release, one question open to deliberation is whether the monitoring techniques employed by probation officers infringe on offenders' expectations of privacy under the Fourth Amendment.[14]

The comment argues that current technological monitoring techniques used to track the computer activities of convicted child pornographers do not constitute a violation of Fourth Amendment search

---

[8] *Compare* United States v. Granger, 117 F. App'x 247 (4th Cir. 2004) (upholding a special provision restricting defendant's use of computers to those without Internet access, without allowing a probation officer's exception), *with* United States v. Holm, 326 F.3d 872 (7th Cir. 2003) (holding that a total ban on Internet use as a condition of defendant's supervised release was too broad and unnecessarily deprived the defendant's liberty).

[9] *See* cases, *supra* note 8.

[10] *See* United States v. Sofsky, 287 F.3d 122 (2d Cir. 2002); *see also* United States v. Freeman, 94 F. App'x 40 (3d Cir. 2004).

[11] United States v. Knights, 534 U.S. 112, 119 (2001) (quoting Griffin v. Wisconsin, 483 U.S. 868, 874 (1987), in turn quoting Morrissey v. Brewer, 408 U.S. 471, 480 (1972)).

[12] *See supra* note 11, for cases that acknowledge the forfeiture of certain First and Eighth Amendment rights for parolees who have relinquished full protection by virtue of their parolee status after conviction.

[13] This comment addresses the practicality of enforcing a total Internet ban in section II.

[14] *See infra* note 49 for a discussion of this point in United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004).

and seizure entitlements. Thus, Fourth Amendment concerns do not prevent a court from imposing a condition during sentencing that allows an offender some Internet access through monitoring software that tracks online activity. However, attempts to police the online activity of those offenders implicate public policy issues, including re-training costs which arise when probation officers learn how to enforce the restriction. These concerns render the probationary restrictions both problematic to employ and difficult to enforce.

This comment evaluates the efficacy of the current probation punishment scheme to conclude that punishment solely by the terms of probation or parole violations is inadequate. In response, the comment proposes that circumventing government efforts to make safe a technology following a conviction for viewing, possessing, or distributing online child pornography should invoke an additional, independent civil and criminal offense. The comment first addresses probation as a form of punishment and how different courts of appeals historically approached a restriction on Internet access as a condition of supervised release in the context of the Fourth Amendment. The next section discusses the impracticality of imposing a total Internet ban on sex offenders. The third section explains current computer surveillance techniques the government employs to monitor offenders in jurisdictions that limit Internet access. The fourth section presents the problems of practicality that accompany enforcement of restricted Internet access in the probationary context. The fifth section analyzes the credibility problem that effectively renders a violation of probation an empty threat. Using the Digital Millennium Copyright Act as a model,[15] the final section discusses the rise of criminal copyright infringement to propose a statutory scheme that creates criminal and civil penalties for those offenders who circumvent the software used to restrict Internet access as a condition of probation.

II. PROBATION AS PUNISHMENT FOR INTERNET CRIMES

A. Probation and Supervised Release Under the Sentencing Guidelines

Conditional restrictions are authorized by statute as a form of punishment after conviction under a scheme of supervised release or probation within the United States Sentencing Guidelines ("Guidelines").[16] In addition to providing a calculus for actual time in prison, the Guidelines also inform a judge's decision to impose a term of

---

[15] 17 U.S.C. § 1201 (2006).
[16] 18 U.S.C. § 3583 (2006).

supervised release to follow any prison sentence, or allow the defendant to return to society for a term of probation subject to attached conditions.[17]

Supervised release is allowed only under certain conditions outlined in the Guidelines.[18] Unlike parole, which merely shortens the amount of prison time served, supervised release is a period of time following the full term of incarceration.[19] While the length of supervision varies depending upon the underlying crime, section 3583 indicates that supervision cannot exceed five years for severe crimes.[20] These conditions of release contain both mandatory and discretionary provisions, permitting a judge to order further restrictions on an offender who obtains supervised release.[21] The Guidelines employ a balancing approach to ensure that a sentence imposes no greater deprivation than necessary to afford an offender the opportunity to rehabilitate while simultaneously protecting the public against recidivism by meeting penal goals.[22]

A court imposing a discretionary condition of supervised release or probation must ensure that the condition is reasonably related to the factors set forth in section 3553, including: the nature and circumstances of the offense;[23] the need for the sentence imposed, incorporating the seriousness of the offense and the interest in promoting respect for the law while providing just punishment;[24] the deterrence of further criminal conduct by the defendant;[25] and the protection of the public from further criminal conduct by the defendant.[26] Furthermore, the condition must involve "no greater deprivation of liberty than is reasonably necessary"[27] for the purposes of deterrence and protection of the public while remaining consistent with policy statements issued by the Sentencing Commission for any condition set forth as a discretionary condition of

---

[17] *Id.*

[18] *Id.*

[19] Christopher Wiest, Comment, *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 (2003). The Supreme Court's decision in United States v. Booker, 543 U.S. 220 (2005), rendered the Guidelines merely advisory instead of mandatory in the Federal system, permitting judges a greater degree of discretion during sentencing.

[20] 18 U.S.C. § 3583(b) (2006).

[21] 18 U.S.C. § 3583(d).

[22] Wiest, *supra* note 18, at 850.

[23] 18 U.S.C. § 3553(a)(1) (2006).

[24] § 3553(a)(2)(A).

[25] § 3553(a)(2)(B).

[26] § 3553(a)(2)(C).

[27] United States v. Heidebur, 417 F.3d 1002, 1004 (8th Cir. 2005).

supervised release or probation.[28] Hence, courts are cognizant of remaining within the parameters of the Guidelines when imposing Internet restrictions as a condition of supervised release or probation for sex offenders convicted of trafficking online child pornography.

B. Appellate Courts Differ in the Treatment of a Restriction on Internet Access as a Condition of Supervised Release or Probation

The courts of appeals differ in their evaluations of district court decisions that employ the option of sentencing offenders to supervised release or probation with restrictive conditions after convictions for Internet crimes.[29] District courts rely on an ability to impose discretionary special conditions in order to restrict an offender's access to the Internet after a conviction for trafficking online child pornography.[30] Appeals to such conditions historically met with different results, creating a split among the courts of appeals regarding the propriety of a denial to Internet access.[31] The Ninth and Eleventh Circuits have upheld conditional restrictions on Internet usage for individuals convicted of sex crimes, while the Second and Eighth Circuits have reversed Internet restrictions as conditions of supervised release.[32] Different courts of appeals historically addressed restricting

---

[28] § 3553(a)(4)(B).

[29] *See supra* notes 6 and 8 for examples of different appellate court rationales in the probationary setting. In addition, as of September 2007, the Tenth Circuit split with the Third and Fifth Circuits regarding a presumption of transmission across state lines when defendants use the Internet. *Compare* United States v. Schaefer, 501 F.3d 1197 (10th Cir. 2007) (reversing the district court to hold that there is no presumption that an Internet transmission, standing alone, moves across state lines to satisfy the interstate commerce requirement in the federal child pornography statute [18 U.S.C. § 2252(a) (2006)]), *with* United States v. MacEwan, 445 F.3d 237 (3d Cir. 2006) *and* United States v. Runyan, 290 F.3d 223 (5th Cir. 2002) (both allowing the government to satisfy the requisite interstate commerce nexus through direct evidence of a defendant's Internet use).

[30] 18 U.S.C. § 3553 (2006).

[31] For example, the Fourth Circuit in United States v. Granger, 117 F. App'x 247 (4th Cir. 2004), denied a defendant the use of any computer with Internet access, while the Seventh Circuit, in United States v. Holm, 326 F.3d 872 (7th Cir. 2003), recognized the defendant's liberty interest to allow him Internet access.

[32] *Compare* United States v. Rearden, 349 F.3d 608, 621 (9th Cir. 2003), *and* United States v. Zinn, 321 F.3d 1084, 1093 (11th Cir. 2003) (both upholding an Internet restriction), *with* United States v. Crume, 422 F.3d 728, 733 (8th Cir. 2005) (reversing an Internet restriction), *and* United States v. Sofsky, 287 F.3d 122, 126 (2d Cir. 2002) (reversing an Internet restriction). In June 2007, the Third Circuit vacated conditions of supervised release against a defendant that imposed an absolute lifetime ban on using computers and computer equipment with no exception for employment or education, coupled with a permanent ban against possession of "sexually explicit" books, movies, or video games. *See* United States v. Voelker, 489 F.3d 139, 145 (3d Cir. 2007) (noting that the condition's permanency was "the antithesis of a 'narrowly tailored' sanction" and that "[t]he ubiquitous presence of the [I]nternet and the all-encompassing nature of the

Internet access as a condition of supervised release in the context of the Fourth Amendment.[33]

In 1999, the Third Circuit in *United States v. Crandon*[34] was the first to address a restriction on Internet access. The defendant was convicted of receiving child pornography and challenged a condition of his probation that denied him access to the Internet unless he sought specific approval from the United States Probation Office.[35] The court upheld the restrictive condition, considering it reasonably related to the caliber of the defendant's offense and the government's goal of protecting the public.[36]

Two years later, in *United States v. Paul*, the Fifth Circuit affirmed a blanket prohibition against Internet access for a defendant whose computer contained over 1,200 images of child pornography and who used e-mail to advise others on how to gain access to children by targeting single parents.[37] The court accepted a broad restriction that did not include a provision permitting the defendant to use the Internet with approval of his probation officer.[38] The Fifth Circuit also rejected the defendant's argument that the Internet had become an indispensable tool for communicating in the modern world.[39]

In contrast, other appeals courts hesitate to embrace restrictions on Internet access. In *United States v. White*,[40] the Tenth Circuit commented that the ban imposed there could be acceptable under circumstances

---

information it contains . . . provides near universal access to newspapers such as the *New York Times*; the *Wall Street Journal* and the *Washington Post*; to popular magazines such as *Newsweek* and *Time*, [to] such respected reference materials as the Encyclopedia Britannica and World Book Encyclopedia, and [to] much of the world's literature."). One commentator noted that when read literally, the condition would have prohibited the defendant from ever owning a modern mobile phone or many books including the Bible, medical textbooks, and modern fiction classics. *See* Declan McCullagh, *Police Blotter: Court Overturns Man's Net Ban for Life*, CNET, June 6, 2007, *available at* http://www.news.com/Police-Blotter-Court-overturns-mans-Net-ban-for-life/2100-1030_3-6188973.html.

[33] *See, e.g.*, United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004); United States v. Holm, 326 F.3d 872 (7th Cir. 2003).

[34] United States v. Crandon, 173 F.3d 122 (3d Cir. 1999).

[35] *Id.* at 125. Crandon pled guilty to one count of receiving child pornography in violation of 18 U.S.C. § 2252(a)(2) and was later sentenced to seventy-eight months in prison followed by a three-year term of supervised release.

[36] *Id.* at 128. The court indicated that the restrictive condition was narrowly tailored and consistent with the defendant's criminal conduct even though it jeopardized his employment and impacted his First Amendment freedoms, because Crandon had used the Internet to develop and exploit an illegal relationship with a fourteen-year-old girl.

[37] United States v. Paul, 274 F.3d 155 (5th Cir. 2001), *aff'd*, 122 S. Ct. 1571 (2002).

[38] *Id.*

[39] *Id.* at 169–70.

[40] 244 F.3d 1199 (10th Cir. 2001).

evident in *Crandon*.[41] However, the court remanded the special condition in its own case back to the district court so that it could be reworded "to reflect the realities of the Internet and its rapidly changing technology."[42] The court found that the special condition was overly broad and potentially violated the Sentencing Guidelines by imposing a restriction "greater than necessary,"[43] which denied the defendant's use of "a computer at a library to do any research, get a weather forecast, or read a newspaper online."[44]

Building on a concern to tune the scope of restrictive probationary Internet conditions, the Second Circuit invalidated a special condition in 2004 that required the defendant to submit to electronic monitoring of his computer by his probation officer in *United States v. Lifshitz*.[45] Noting that such a condition may be reasonable in certain circumstances, the court indicated that the current monitoring scheme was overbroad as imposed.[46] The court performed a Fourth Amendment analysis to conclude that the "special needs" of the probationary system[47] justified conditioning the offender's probation upon his agreement to submit to computer monitoring.[48] However, the Second Circuit in *Lifshitz* held that the broad wording of the probationary condition rendered an analysis of infringement on the defendant's privacy impossible, since the court record provided little information as to the specific system intended to monitor or filter the computer.[49] Furthermore, the court questioned the efficacy of such enforcement techniques, recognizing that experienced computer users might circumvent the software, thus reducing the effectiveness of the government's justification for implementing those measures.[50]

In sum, the Third and Fifth Circuits split from the Second and Tenth Circuits within a Fourth Amendment justification scheme when evaluating the scope of restrictive online access imposed by the district

---

[41] The *White* court explained that Crandon's use of the Internet "clearly initiated and facilitated a pattern of criminal conduct and victimization that produced an immediate consequence and directly injured the victim," and noted that Crandon could still access the Internet with permission from his probation officer. *Id.* at 1205. *See supra* note 34.

[42] *Id.* at 1206.

[43] 18 U.S.C. § 3553(a) (2006).

[44] *White*, 244 F.3d at 1206.

[45] 369 F.3d 173 (2d Cir. 2004).

[46] *Id.*

[47] The "special needs" were to rehabilitate the defendant and ensure that he did not harm the community further by receiving or disseminating child pornography during his term of probation. *Id.*

[48] *Id.* at 190.

[49] *Id.* at 193.

[50] *Lifshitz*, 369 F.3d at 193.

courts. Courts must tailor the language in each restrictive condition using authority from the Sentencing Guidelines to acknowledge each offender's Fourth Amendment privacy concerns.

C. The Fourth Amendment Does Not Bar Internet Restrictions for Sexual Offenders Sentenced to Probation

This comment proposes that a restriction on Internet access is a valid option for any district court sentencing a convicted sex offender to probation. However, the existing circuit split illuminates two issues. First, courts must evaluate the degree of any imposed Internet restriction in the context of each defendant's Fourth Amendment rights to ensure that the denial is no more than necessary. Second, the courts then must consider whether the subsequent monitoring techniques put into place by the probationary condition deny the offender any Fourth Amendment guarantees against unreasonable searches.

1. Internet Restrictions as Conditions of Supervised Release Do Not Violate the Offender's Fourth Amendment Right to Privacy

Though circuit courts split their decisions about the extent of restricting the Internet for sex offenders who traffic in online child pornography, the restriction itself does not pose any threat to the offender's Fourth Amendment privacy rights against unreasonable searches and seizures. This is permissible because courts can tailor each restriction to comport with privacy concerns in any given situation. The split among circuit courts begins with imposition of a total or partial ban on Internet access as a condition of probation or parole, and further deepens the Fourth Amendment analysis for those courts that choose the partial ban allowing limited Internet access. Courts that impose a blanket prohibition on Internet access, like the Fifth Circuit in *Paul*, appear to focus wholly on the Guidelines by rationalizing that the egregious quality of child pornography validates the propriety of a total ban.[51] Comparatively, courts of appeals reviewing conditions that allow partial Internet access through restrictive computer monitoring measures address an additional Fourth Amendment component when analyzing a probationary special condition. These courts must ensure that the scope of partial access comports with the privacy rights of the defendant while simultaneously complying with the principles that drive the Sentencing Guidelines.[52]

---

[51] *See* United States v. Paul, 274 F.3d 155 (5th Cir. 2001).

[52] The court's analysis in *United States v. Lifshitz*, 369 F.3d 173, 191 (2d Cir. 2004) illustrates this task.

2. Under the Supreme Court's Existing Jurisprudence, Computer Searches Based Wholly on Probationary Status Would Likely Not Violate the Fourth Amendment

While the Supreme Court has never addressed the question of whether a warrantless search is reasonable under the Fourth Amendment if the search were solely predicated upon the condition of probation,[53] the Court's jurisprudence suggests that searches based on probationary status alone likely do not violate the Fourth Amendment.[54]

In *Samson v. California*, the Supreme Court relied on a prior decision in *Griffin v. Wisconsin* to assess a case involving a suspicionless search of an offender out on parole.[55] In *Griffin*, the Court acknowledged the special role of probation officers: "[W]e deal with a situation in which there is an ongoing supervisory relationship—and one that is not, or at least not entirely, adversarial—between the object of the search and the decisionmaker."[56] The *Samson* Court incorporated that rationale and ultimately held that the Fourth Amendment did not prohibit a police officer from conducting a suspicionless search of a parolee based solely on parolee status, suggesting that a condition of supervised release can eliminate an offender's reasonable expectation of privacy.[57] The Court noted that parole grants offenders a privilege premised upon compliance with other requirements.[58]

Moreover, the *Samson* Court cited special conditions for parolees, such as psychiatric treatment and mandatory abstinence from alcohol, as examples of a parolee's limited expectation of privacy based on parolee status alone.[59] Akin to probationers, the Court considered the defendant's compliance with the parole option to be an equally "salient" factor, evidencing personal awareness and acceptance that he might be subjected to suspicionless searches.[60] Consequently, the Court concluded that "imposing a reasonable suspicion requirement [before police officers could search parolees] would give parolees greater opportunity to anticipate searches and conceal criminality."[61] The Court concluded that concerns about an offender's incentive to conceal contraband merited an

---

[53] *Knights*, 534 U.S. 112, at 120.

[54] *See* Griffin v. Wisconsin, 483 U.S. 868 (1987); Samson v. California, 126 S. Ct. 2193 (2006).

[55] *Samson*, 126 S. Ct. at 2199.

[56] *Griffin*, 483 U.S. at 879.

[57] *Id.* at 879–80.

[58] *Samson*, 126 S. Ct. at 2198 (citing Pennsylvania Bd. of Probation & Parole v. Scott, 524 U.S. 357, 365 (1998)).

[59] *Id.* at 2199.

[60] *Id.*

[61] *Id.* at 2201. *See Knights*, 534 U.S. at 120; *Griffin*, 483 U.S. at 879.

"intensive" system of supervision in *Griffin v. Wisconsin*, and that these concerns applied with even greater force to the supervision of parolees.[62]

Consequently, while the Supreme Court's existing jurisprudence does not explicitly address a condition of probation that restricts probationer or parolee access to the Internet, it sets a framework that allows the inference that the Fourth Amendment is not implicated in such instances. Incorporating the adversarial supervisory relationship of probation officers and offenders acknowledged in *Griffin* into *Samson*'s limited rights rationale implies that Fourth Amendment rights are not violated when courts restrict Internet access to offenders granted supervised release or probation.

III. ENFORCEMENT OF A TOTAL BAN ON INTERNET ACCESS IS PROBLEMATIC AND IMPRACTICAL

Despite diminished Fourth Amendment concerns, a court still faces the task of drafting a suitable restrictive condition for an offender living in a technologically-dependent society. A court considering a condition of probation must acknowledge the realities of the Internet age while effectively limiting the offender's computer activity.[63] Circuit courts allowing restrictive access to the Internet need to uphold the Sentencing Guidelines by narrowly tailoring special conditions. Conflicting circuits that promote a total ban on Internet access face additional problems of practicality when enforcing the blanket prohibition.

Internet technology is so commonplace and convenient that curbing offender access seems nearly impossible.[64] The ease of online accessibility creates a huge burden on law enforcement when both the public and private sectors offer Internet access so readily—nearly every public library and airport offers computers with Internet access, and most cellular phones now have online capability. Furthermore, hotel rooms, gyms, and educational institutions provide countless opportunities for crafty offenders to violate a blanket prohibition on Internet access. Technological change is so rapid that it is possible to contemplate easier means of Internet access in the future, even in areas that have yet to succumb to the digital network.[65] A complete bar to online access also affects the sentencing goal of rehabilitation—probationers are expected

---

[62] *Samson*, 126 S. Ct. at 2201; *Griffin*, 483 U.S. at 875; *see also* United States v. Reyes, 283 F.3d 446, 461 (2002).

[63] The Tenth Circuit majority made such an acknowledgment in *United States v. White,* 244 F.3d 1199, 1207 (10th Cir. 2001).

[64] *See* Where Americans Use the Internet, http://www.infoplease.com/ipa/A0921870.html (last visited Sept. 15, 2007).

[65] Some examples include automatic Internet capability wired into every new home, or free wireless signals on buses or subway systems and in waiting areas of hospitals.

to secure steady employment, but may be wary of pursuing many clerical jobs in contemporary society that now offer Internet access. In addition, employers and potential employees alike utilize online research and communication resources related to the job search. While not a perfect solution, however, blocking software may justify a partial ban to restore the Internet as an acceptable tool a probationer may use to obtain employment.

The anonymity of the electronic interface is another factor that precludes effective enforcement of a total Internet ban. Although Internet access in the employment context is more readily regulated because employers can bar any probationer from using a computer or going online, private circumvention of the probationary condition is easily achieved if offenders merely borrow computers or choose different login names. The previous section argues that offenders cannot protest a complete ban on the principle that the Internet's indispensability dictates them a right to read a newspaper or book travel arrangements online, because the "unfairness" argument implicates a quality-of-life assertion that probationers and parolees are no longer qualified to make. *Samson* and other Supreme Court precedent diffuse the argument that because the Internet is so pervasive, any denied access to it implicates Fourth Amendment concerns. The rationales put forth by the Supreme Court in *Samson* and *Griffin* indicate that probationers and parolees simply do not enjoy the same constitutional entitlements as regular citizenry because of criminal conduct.[66] Sex offenders convicted for abusing the Internet therefore should not expect a right to use it, especially when their criminal conduct hinged entirely on the technology.

On the other hand, if offenders protest that a condition against total Internet access is unfair and impractical this contention may be valid when there is a risk for violation through Internet exposure that is not within their control, such as at a library, airport, or gym. The ban is designed to prevent actual Internet activity, however, and most of these exposures would require further conduct on the offender's part. Still, the daily infusion of Internet technology presents many potential opportunities for an offender to violate probation and law enforcement's limited ability to enforce a ban cannot completely alleviate the risks from an environment rife with temptation.

All courts that contend with sex offenders convicted of trafficking child pornography on the Internet seek to satisfy the Sentencing Guidelines by matching punishment to the nature of the crime

---

[66] *Samson*, 126 S. Ct. at 2198 (citing United States v. Cardona, 903 F.2d 60, 63 (1st Cir. 1990)).

committed. The goal of those circuits that impose a blanket prohibition on Internet access is both noble and obvious, but fails to account for the impracticality of enforcing the condition. The Internet's dominant role in society makes monitored restricted access a more viable option for the courts. Therefore, courts intent on restricting Internet access must specify technological measures that impose varying degrees of intrusion.

IV. VARIOUS TECHNOLOGICAL METHODS ARE AVAILABLE TO ENFORCE A RESTRICTION ON INTERNET ACCESS

A survey of current technology highlights the variety of methods available for probation officers to enforce conditions that permit offenders partial Internet access. Current technology allows for flexibility, but also creates opportunities for offenders to circumvent existing methods. Available enforcement measures include installing software on an individual's personal computer and tracking records provided by the probationer's Internet Service Provider ("ISP").[67]

A. Software Technology

Software provides an advantage over ISP record-keeping in that software allows a probation officer or other monitor to investigate all of a probationer's computer-based activities for offensive behavior that might occur without accessing the Internet.[68] Installed software can target specifically-unauthorized materials, or may monitor the computer user's activity in the entirety.[69] The Second Circuit suggested in *United States v. Lifshitz* that "[t]hese [technological] distinctions may be material to determining whether the scope of the monitoring condition's infringement on privacy is commensurate with the 'special needs' [analysis used to determine the validity of a condition of supervised release.]"[70]

The Second Circuit's invalidation of the computer restriction in *Lifshitz* reflected the court's concern that the lack of specificity as to the government's intended means of monitoring might result in a violation of what it held to be Lifshitz's reasonable expectation of privacy. The court explained that "[c]onstant inspection . . . might be more like searching his diary or inspecting his closets than it is like the highly targeted diagnosis accomplished by [a monitoring means similar to] drug testing."[71] The Second Circuit then advocated a monitoring system that

---

[67] United States v. Lifshitz, 369 F.3d 173, 191 (2d Cir. 2004).
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 192.

would alert a probation officer only when the defendant engaged in designated impermissible communication over e-mail or the Internet.[72]

The *Lifshitz* court emphasized that the scope of any online monitoring condition must align with the "special needs" of each defendant's reasonable expectation of privacy.[73] The tools available to law enforcement allow courts to vary the scope of any condition pursuant to a probationary Internet restriction. Probation officers use a variety of software that logs a user's recent computer activity, actively monitors current usage, and filters an offender's access to Internet websites.

1. Forensic Software

Forensic software enables an investigator to collect and recover stored computer data for later analysis of a user's cumulative past activity. Recent technological advancements provide investigators with the option of physically seizing a computer and examining its contents, or alternatively logging into a network that provides virtual access to a user's computer system. The standard tool widely recognized by the industry and validated by the courts is EnCase®.[74] This software is offered in two editions that operate by mounting stored data from the user's drive into an activity log that is accessed by an investigator utilizing a private access key.[75]

The ability of the Enterprise software to run in a live environment differentiates it from the Forensic edition, allowing the investigator to log into a network which makes a virtual connection to a target user's machine that complies with the investigator's request to snapshot volatile data or preview the user's drive.[76] The software encrypts the offender's data and is accessible only to specifically authorized parties, to provide a greater security measure against tampering while establishing a chain of custody that is admissible in court. The Forensic edition provides the same evidentiary activity log, but requires a probation officer to physically access the probationer's computer to retrieve the usage report.[77]

---

[72] *Lifshitz*, 369 F.3d at 192.

[73] *Id.* at 191.

[74] JOHN PATZAKIS, DIGITAL PRIVACY CONSIDERATIONS WITH THE INTRODUCTION OF ENCASE ENTERPRISE (2003), http://www.guidancesoftware.com/downloads/getpdf.aspx?fl=.pdf.

[75] *Id.*

[76] How EnCase® Enterprise Works, http://www.guidancesoftware.com/products/ee_works.asp (last visited Feb. 11, 2007).

[77] PATZAKIS, *supra* note 74, at 2.

2. Monitoring Software

Continual monitoring software such as SPECTOR® can supplement a periodic review of past computer usage. Monitoring software captures the user's entire computer by recording all computer activity including Internet browsing and web-based e-mail services such as Hotmail, Yahoo mail, and AOL.[78] This monitoring program takes a snapshot of a person's computer use as frequently as once per second, holding usage information accrued over several months in a hidden location for later review by an outside party.[79] The automatic snapshot function mimics a surveillance camera by providing a visual record of screenshots, while recording e-mail, chat conversations, and user keystrokes.[80] The Professional edition of the software e-mails an immediate report to a designated recipient once the offender uses any inappropriate keywords delineated in advance by the subscriber.[81] This notification report contains details of when, where, and how a keyword was used, including the number of times it was typed or appeared on a computer, on a website, or in an e-mail.[82]

3. Filtering Software

Software can filter or block information on an offender's local computer or function through an ISP to block user access to predetermined websites as a probation officer dictates per the terms of probation. Proxy server programs control network traffic between local users and the Internet. A probation officer can designate settings that deny specific file requests from a local user or block inappropriate web pages and e-mail messages.[83] For example, the *Lifshitz*[84] opinion noted in dicta how an off-site ISP in Bexar County, Texas maintained an agreement with the local judiciary, providing probationers with Internet service that restricted access to sex-related sites or other areas expressly forbidden by conditions of parole or probation.[85] The system provides an alternative software method by interrupting Internet data at the ISP

---

[78] Spying & Detective Software Reviews and Download Page!, http://www.webtechgeek.com/Spy-Software.htm (last visited Feb. 11, 2007).

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] Proxy Server, http://www.webopedia.com/TERM/p/proxy_server.html (last visited Dec. 27, 2007).

[84] *Lifshitz*, 369 F.3d at 191 (discussing Ihosvani Rodriguez, *Three Sex Offenders Caught Seeking Internet Porn; Trio Had Agreed To Be Under the Authority of Cyber-Watchdogs*, SAN ANTONIO EXPRESS-NEWS, Dec. 28, 2001, at 1A.).

[85] *Id.*

source rather than via screenshot monitoring or pre-access blocking methods. All technologies require a skilled probation officer to program or sort through the resultant data and require strategic planning to keep pace with resourceful offenders who may attempt to circumvent each technology. Thus, when tailoring release conditions, courts select from a technological menu with varying degrees of surveillance options including activity logs, screen snapshots, and interruptive filtering of network traffic. Courts must also consider the technological proficiency of each offender to reduce the potential for circumvention.

B. Flexibility in Software Options Mitigates Potential Privacy Concerns in the Probationer Context

Just as a court can customize probationary conditions to reduce privacy concerns when restricting Internet access, applicable methods of monitoring and restricting are flexible enough to allow custom tailoring of any probationary condition. Forensic software focuses on past behavior, and while physical acquisition of an offender's computer adds an intrusive element, designating a method such as remote accession to preview a target drive permits narrow tailoring of a probationary condition. A probation officer's ability to search for particularized illegal activity within a designated computer closely matches the *Lifshitz* guidelines, further mitigating Fourth Amendment protests from probationers subject to restricted Internet access.

C. Skilled Internet Offenders Invite the Potential for Circumvention

While the Fourth Amendment poses no great hurdle to Internet restrictions, an unwieldy Internet landscape complicated by the technological prowess of particular offenders threatens every method of computer surveillance with the potential for subversion. Given the ever-changing breadth of sexually-related content available online, probation officers face the impractical task of staying abreast of myriad pornographic sites that morph and change on a daily basis in order to effectively program the filtering software.[86] An offender might defeat monitoring through encryption or steganography, both of which entail hiding trigger messages within a larger document.[87] Moreover, the proliferation of free proxy websites allows any computer user to hide a

---

[86] ISC Internet Domain Survey, http://www.isc.org/index.pl?/ops/ds/ (last visited Sept. 15, 2007) (Internet Domain Name survey indicates over 500 million current online host sites as of January, 2007).

[87] Jim Tanner, *Rethinking Computer Management of Sex Offenders Under Community Supervision*, 15 J. OFFENDER MONITORING 11, (Summer/Fall 2002), *available at* http://www.kbsolutions.com/rcm.pdf.

personal IP address and surf the Internet anonymously without revealing the identity of the particular computer.[88] Alternatively, offenders can simply utilize a non-monitored computer to circumvent any condition of probation. Thus, the various technologies available provide flexible options but do not resolve the circumvention problem. These realities reinforce the pressing need for additional deterrents such as specific statutory civil and criminal penalties for any user who willfully circumvents monitoring or filtering technology installed as a restrictive condition of probation.

V. ENFORCEMENT OF A PARTIAL BAN ON INTERNET ACCESS IS POSSIBLE YET ULTIMATELY PROBLEMATIC

While Fourth Amendment concerns are reduced for those subjected to partial Internet bans because the judiciary can adjust probationary conditions for any situational need, attempts to police the online activity of those offenders invoke the same practical obstacles that arise out of the total ban scenario. Regardless of the technological method employed, monitoring the Internet habits of probationers implicates public policy issues relating to cost, officer qualifications, and practicality, given the ease of Internet access in daily life and the constant volatility in content. There are transactional costs that will accompany any monitoring or filtering method employed with Internet restrictions as a condition of probation. For example, probation officers must be trained to effectively enforce the Internet restriction. Proper preparation may demand an entirely new skill-set of technological awareness. For those courts that do not restrict Internet access due to its prevalence in today's society, the practicality of enforcing special probationary conditions becomes an issue after a sentence grants law enforcement access to an offender's computer.

A. Enforcing an Internet Restriction is Impractical Because the Internet is Easily Accessible

The proliferation of Internet use within public space makes enforcement of a probationer's Internet access potentially unwieldy. Monitoring and filtering are only useful for activities conducted on a designated computer. Compliance with an Internet restriction creates an additional challenge for probationers who may be employed in jobs that require the use of a computer. Further, Internet access is readily available from public computers at the public library or even via online access through cellular phones. New York City has currently contracted with an

---

[88] *See*, *e.g.*, http://www.WebsiteProxy.org; http://www.proxytopsite.com.

Internet Service Provider to make Central Park a hotspot with free wireless Internet access.[89]

The effects of restricting the Internet for a probationer are useless if the user cannot be identified when using a different computer. Techniques will accommodate this truth in ways that affect greater society. Enforcing a restriction by blocking access to specific sites at the public library, for example, might deny the general public fair use simply because of a potential for abuse by probationers and parolees.[90] The resultant public policy would create a perversely tightened and restrictive Internet environment for the masses who have not voluntarily relinquished rights through the commission of a crime.

B. Enforcing an Internet Restriction is Difficult Because Technology is Volatile

The limitations of current technology cannot always satisfy the judicial scope of Internet monitoring in conditions of probation or parole, further reducing the efficacy of restrictive conditions. While courts may craft monitoring conditions of probation that satisfy the jurisprudential scope of an Internet restriction, actual implementation is unwieldy and impractical. Proponents of the Internet ban as well as its detractors agree that the development of forensic search technology is uncertain at best and subject to immediate counter-strategies devised by savvy hackers.[91] The sheer number of rapidly changing forensic programs further complicates the practicality of enforcing an Internet ban.[92] The best tool for a particular situation greatly depends on its cost and ease of use, as well the skill of the particular officer using it.[93]

C. Adequately Enforcing an Internet Restriction Often Requires Specialized Training for Probation Officers

Offenders may possess computer knowledge that far surpasses that of their probation officers. This invites a game of "cat-and-mouse"[94] to epitomize the potential futility of relying on technological methods to

---

[89] Sewall Chan, *Deadline Set for Wireless Internet in Parks*, N.Y. TIMES, May 16, 2006, at B1.

[90] Arguably, the general public could be denied access to sites that are not pornographic in nature but are nevertheless blocked to prevent access to probationers because the sites contain images of children or offer particular items for sale.

[91] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 570 (2005) (referring to computer hackers who have the technological prowess to immediately circumvent new monitoring techniques).

[92] *Id.*

[93] *Id.* at 579.

[94] *Id.* at 570.

adequately enforce an Internet restriction. Thus, monitoring and filtering the Internet for probationers and parolees by permitting such individuals to live outside of prison introduces a new task of balancing the price of enforcement against the dual goals of deterrence and rehabilitation where individual privacy and public safety is no longer the primary issue. By relaxing Fourth Amendment concerns for probationers and parolees, courts remove the dreaded fact-finding burden that would require them to cull the latest technologies in order to prescribe the least-invasive monitoring techniques for a probationary condition of release. Courts also avoid the potential for a clogged judiciary when defendants like Lifshitz return to court to request modifications to supervisory conditions in the face of cutting edge technology that would reduce an infringement on their Fourth Amendment rights. In order to impede an offender's potential to violate the Internet restriction, conditions should clearly mandate that the offender use only specially-designated computer terminals, perhaps in conjunction with random drop-in visits and continual technological surveillance by probation officers.

1. The Colorado Training Scenario

The state of Colorado spearheaded an effort to develop an intensive two-day technical training program for probation officers at the Rocky Mountain location of the National Law Enforcement and Corrections Technology Center ("NLECTC-Rocky Mountain").[95] The course builds on the notion that there is no known cure for sexual deviancy and furthers the goal of containing an offender's deviant impulses by using programs that help identify thinking errors, recognize risk factors in the environment, and develop skills to control online behavior.[96] The training teaches officers how to frame the conditions of probation to allow the probation agency the right to search an offender's computer at any time.[97] The program coincides with a writing in which the offender agrees not to view pornographic materials online and concedes that he is responsible for any data found on the computer.[98] The computer user signs a form that indicating that "(s)he has "no expectation of privacy regarding all computer use and/or information stored on his/her

---

[95] *"Monitoring" the Sex Offender*, TECHBEAT, Winter 2005, at 5, *available at* http://www.nlectc.org/pdffiles/tbwinter2005.pdf.

[96] *Id.*

[97] Michelle Gaseau, *Sex Offender Supervision and Technology*, CORRECTIONS CONNECTION NETWORK NEWS, June 13, 2005, *available at* http://corrections.com/news/article/5000.

[98] *Id.*

computer."[99] This scheme employs a contract theory of law between the government and the probationer, the "consideration" being probation instead of jail or an accepted shorter jail term in exchange for conditional supervised release.

The NLECTC-Rocky Mountain also provides free software for probation officers to detect electronic violations of probation.[100] The software reviews an offender's hard drive and generates reports that are admissible in court and can be printed or e-mailed to others.[101] In addition, the officer learns to apply a treatment review protocol to manage the offender under the supervision goals established within the initial agreement.[102] The offender is continually mapped for adaptive treatment in an effort to prevent the offender from misdirecting the supervision team over time.[103] Officers participating in the program install monitoring software on the offender's computer which scans and captures photographic images and text, generating a report before the officer wipes the computer as a blank slate for the next scanning session.[104] However, while officers learn the basic capability of forensic software to track offender activity, they are not trained to recognize technical circumvention of any particular monitoring program.

Contrary to the traditional law enforcement approach to computer forensics which treats a hard drive as a historical record of evidence for a crime that has already occurred, probation and parole officers are oriented to approach the offender's computer usage with methods of monitoring to prevent repeated crime.[105] Software runs periodic checks of the hard drive to determine if there has been any violation of the probationary condition or if a new crime has been committed.[106] The driving principle behind this method parallels the rationale behind drug testing, which theorizes that while offenders may beat a particular instance of computer monitoring, users who continue to violate will eventually get caught.[107]

The added cost to train and qualify probation officers to handle the particular demands of the sex offender Internet probationary condition

---

[99] To view the complete terms of a sample agreement, *see* http://www.kbsolutions.com/intakeagr.pdf.

[100] Gaseau, *supra* note 97.

[101] *Id.*

[102] KB Solutions, Structured Sex Offender Treatment Review Overview, http://www.kbsolutions.com/html/ssotr.html (last visited Feb. 11, 2007).

[103] *Id.*

[104] Gaseau, *supra* note 97.

[105] *Id.*

[106] *Id.*

[107] *Id.*

signals one obvious drawback of the Colorado model. The "cat-and-mouse" analogy animates the constant evolution of technology, where offenders frequently have more computer literacy than those monitoring them, increasing their prowess by exchanging ideas and methods to dodge monitoring during time spent in prison or through other networks.[108] Additionally, while probation officers are comfortable understanding the personal factors from any one case that may lead to criminal behavior, the Internet contains many unorthodox dangers that complicate the risks each officer must manage. Joe Russo, program manager for corrections at the NLECTC-Rocky Mountain, elaborated in one article that "[o]fficers are used to dealing with offenders' addictions, joblessness, and family relationships; now they must also deal with online pornography, sex chat rooms and discussion boards, and dating services that target vulnerable, single-mom families with the 'right type' of children in the household."[109]

2. The Cost of Training Probation Officers Inhibits the Efficacy of a Probationary Condition

The NLECTC-Rocky Mountain began offering its courses without fees in 2004, but many interested out-of-state agencies did not have the travel budget necessary to send officers to the training site.[110] The current program offers training throughout a ten-state region to key agencies and participants that can provide appropriate computer labs.[111] As of summer 2006, more than 440 probation officers in sixteen states received training.[112] Although regional training consolidated part of the costs to prepare probation officers for their task of monitoring sex offenders in this instance, economic factors surrounding restrictions on Internet access will spur additional public policy analysis within the circuit courts.[113] Enforcing an Internet ban as part of a probationary condition for a sex offender creates many difficulties in actually controlling offender behavior while implicating policy concerns of cost and efficiency. Therefore, the criminal justice system cannot rely on probationary conditions alone to adequately deter and punish these criminals. Limited bans are possible, but not practical, due to the volatility and availability of the Internet and the costs for training

---

[108] *Id.*

[109] *"Monitoring" the Sex Offender*, *supra* note 95.

[110] *Id.*

[111] *Id.*

[112] *Training for Tracking*, TECHBEAT, Summer 2006, at 4, *available at* http://www.nlectc.org/pdffiles/tbsummer2006.pdf.

[113] *See infra* note 177, regarding the anticipated chilling effects of Internet regulation.

probation officers to enforce judicially-imposed conditions. Additional statutory civil and criminal penalties are necessary to thwart offender circumvention problems not resolved by technological monitoring measures.

VI. PUNISHMENT SOLELY BY THE TERMS OF A PROBATIONARY CONDITION IS NOT ADEQUATE

Theoretical analysis and statistical data indicate that probationary conditions are not effective psychological deterrents for many criminals.[114] Consequently, a new model of punishment is necessary to bolster the repercussions that follow a conviction for trafficking child pornography on the Internet. The circumvention sanctions in the Digital Millennium Copyright Act[115] provide a viable sample punishment regime that punishes as a separate crime any effort to circumvent detection. Following this model of intellectual property law, the analysis below offers several reasons why offender activity that circumvents the government's filtering or monitoring efforts to make safe computers should be treated as an additional and independent civil or criminal offense. The consequences for probationers who circumvent monitoring or filtering software are not likely to include incarceration. Hence, probation as a sole remedy suffers from a credibility gap that would benefit from additional independent statutory punishments to boost its deterrent power.

A. Violators of an Internet Restriction as a Condition of Probation Are Unlikely to Face Prison

In general, offenders who violate imposed conditions of probation, or parole under supervised release suffer consequences that are equal to or less than the original crime committed.[116] A term of probation or supervised release commences when the sentence begins.[117] Probation officers have statutory authorization to petition for revocation of probation[118] for any violation of a probationary condition that occurs at any time before completion of the probationary term.[119] Depending on the nature of the violation, the Sentencing Guidelines permit the

---

[114] *See infra* note 136.
[115] 17 U.S.C. § 1201 (2006).
[116] *See, e.g.*, 18 U.S.C. § 3583(b)(1) (2006) (indicating a maximum authorized term of five years of supervised release after conviction for a Class A or B felony).
[117] 18 U.S.C. § 3564(a)-(b) (2006).
[118] 18 U.S.C. § 3603(7) (2006).
[119] 18 U.S.C. § 3564(e) (2006).

sentencing court to revoke probation and impose a prison sentence[120] or to continue probation with the option to extend its term or modify the conditions of release.[121]

When determining a punishment for revocation under the Guidelines, a sentencing court must determine the grade of the violation under section 7B1.1.[122] A judge has discretion to choose the more serious punishment for the crime under either federal or state punishment regimes.[123] Further, courts must grade the violation by taking into account any recidivist provisions a defendant may face if the court charges him with a particular offense.[124] The Sentencing Commission also resolved a circuit split to clarify that where a defendant is sentenced for a new offense after revocation of parole or probation, the district court should impose the new sentence to run consecutively with the revocation sentence. [125]

Courts have some discretion to revoke or revise a defendant's term of probation within the bounds of the Sentencing Guidelines;[126] however, Congress created a basis for mandatory revocation only for offenders who possess firearms, refuse to submit to drug testing, and, most recently, for those who return multiple positive results on drug tests.[127] Accordingly, offenders convicted of child pornography do not face mandatory prison time for the violation of any condition of probation.

B. Probation's Punishment Reputation Suffers from a Credibility Crisis

Current punishment schemes wield threats of increased probation or incarceration if offenders violate conditions of probation, but the criminal justice system suffers from a credibility crisis that feeds probationer recidivism.[128] According to the Center for Civic Innovation at the Manhattan Institute, the criminal justice system's reputation suffers from a lack of legitimacy as perceived by both the general community

---

[120] 18 U.S.C. § 3583(e).

[121] 18 U.S.C. § 3565(a) (2006).

[122] U.S. SENTENCING GUIDELINES MANUAL § 7B1.1 (2006).

[123] *See* United States v. Brennick, 337 F.3d 107 (1st Cir. 2003); United States v. Jolibois, 294 F.3d 1110 (9th Cir. 2002).

[124] *See* United States v. Trotter, 270 F.3d 1150 (7th Cir. 2001); United States v. Boisjolie, 74 F.3d 1115 (11th Cir. 1996).

[125] U.S. SENTENCING GUIDELINES MANUAL § 5G1.3 cmt. n.3(C) (2006).

[126] *Id.*

[127] *See* 18 U.S.C. § 3565(b) (2006); §§ 3565(b)(4) (2002), 3583(g)(4) (2000).

[128] Manhattan Institute for Policy Research, *Transforming Probation Through Leadership: The "Broken Windows" Model*, Civic Report, July 2000, http://www.manhattan-institute.org/html/broken_windows_1.htm (last visited Sept. 30, 2007) [hereinafter *Transforming Probation*].

and the offender.[129] The American population channels its fear and morality into punishment as the centerpiece of policy for crime control.[130] Our societal view is that while punishment and incarceration controls crime, the system should gauge the relativity of threats to public safety and wager accountability for lower-level non-violent offenders via probationary supervision.[131] However, frequent instances of probation violations without sufficient consequence have devalued the public's opinion of probation over the decades.[132] In effect, both society and criminals do not credit the probation system as an effective means of offender deterrence for crime control.

Sheer case volume contributes to the credibility problem—probation officers are overloaded with hundreds of cases to manage, each requiring a varying degree of supervisory control.[133] Many probation departments are under-funded and woefully understaffed with very little interagency cooperation.[134] These logistical impairments result in a certain measure of passivity in case management. Traditional supervision fails to adequately supervise or hold violators accountable, which allows many probationers to avoid meaningful consequences if they violate probationary conditions.[135]

Consequently, many offenders have officially "absconded" by failing to maintain contact with their probation officers, and the system exerts little effort to track absconders or otherwise bring them to justice.[136] For those criminals who agree to follow probationary conditions that attempt to control behavior, there is little public confidence that those offenders will truly be held accountable should

---

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.* Actual monitoring in the community or office monitoring is even less frequent and effective: "Too many probation agencies do not encourage field-based activities providing meaningful face-to-face supervision to offenders in the neighborhoods where they carry on their lives. Probation has become disconnected from such areas, a situation that has resulted in the removal of the 'community' from the business of community supervision." *Id.*

[134] *Transforming Probation*, Civic Report, *supra* note 128.

[135] *Id.*

[136] *Id.* ("[T]en percent of probation violators—about 340,000 persons in 1998—officially 'absconded'. . . . [S]tudies have found that nearly half of all probationers do not comply with the terms of their sentence, and only a fifth of those who violate their sentences ever go to jail for their noncompliance.") (citing T. R. Bonczar & L.E. Glaze, *Probation and Parole in the United States, 1998*, BULLETIN, Washington, DC: Bureau of Justice Statistics, August 1999; and P.A. Langan, *Between Prison and Probation: Intermediate Sanctions*, SCIENCE, May 6, 1994)).

they fail to live up to the prescribed demands.[137] Our system of probation must redefine its image so that probation officers have sufficient credibility to impart a viable threat of punishment as a consequence of violating probationary conditions.[138] Until that point, violators are free to revel in blame, denial of wrongdoing, refusal to accept responsibility, and failure to acknowledge the impact of their behavior on others.[139]

C. Non-Violent Computer Criminals Arguably Perceive Probation's Weaknesses

Though statistics on probationer recidivism focus mostly on violent criminals,[140] the punishment scheme's credibility crisis extends to non-violent offenders who commit computer crimes.[141] Currently, the judiciary tends to impose probation with some form of Internet restriction on child pornographers who trafficked in a low number of offensive images.[142] If this "mild" offender violates a monitoring condition by accessing pornography that is detectable, for example, by a screen capture or by disabling a keystroke monitor, the legal repercussion will likely contain a reprimand and an extension of the term of probation with a tightened monitoring regime. The offender is apt to believe that courts do not want to burden an already overcrowded prison population with a low-level offender, so the violator may capitalize on this vulnerability to exploit it. Thus, the punitive deterrent effect of computer monitoring is arguably lost on low-level offenders.[143]

Further, a facetious attitude toward probationary conditions of this sort potentially infects every incarnation of low-level offender. A technologically illiterate offender familiar with the realities of the criminal justice system might still comprehend that the system is too burdened to imprison him, and so he may consider the possibility of actual punishment for circumventing any computer monitoring an empty threat. Comparatively, an offender who possesses highly sophisticated technical computer knowledge may circumvent monitoring methods based on an arrogance presumption that he can evade detection by

---

[137] *Id.* (referring to results from unspecified public opinion polls).
[138] *Id.*
[139] *Id.*
[140] *See supra* note 136.
[141] *See infra* note 144.
[142] *Compare, e.g.*, United States v. Crandon, 173 F.3d 122 (3d Cir. 1999) (permitting limited Internet access for a defendant convicted of trafficking forty-eight sexually-explicit photographs of a minor), *with* United States v. Paul, 274 F.3d 155 (5th Cir. 2001) (denying the defendant access to the Internet, where his computer contained over 1,200 images of child pornography).
[143] *Transforming Probation*, Civic Report, *supra* note 128.

employing his own software wizardry past his probation officer's sporadic and ineffectual enforcement techniques. Even if this educated offender humbly acknowledges some measure of efficacy from forensic monitoring techniques, he still may share the simpleton's attitude that likelihood of actual punishment is minimal should he choose to access child pornography through the Internet.

D. Alternative Forms of Punishment Are Not Suitable Options for the Non-Violent Computer Criminal

Another judicial remedy is clearly necessary if the punitive threat for violating probation does not intimidate computer criminals into compliance with governmentally-imposed anti-circumvention methods. Because the public seeks more punishment and accountability for offenders, but does not necessarily agree that putting non-violent probation violators in prison is a solution, there remains a paradox of public opinion.[144] Scholars have proposed experimentation with alternative forms of punishment as substitutes for incarceration to broaden the criminal justice system beyond its traditional penitentiary scheme.[145] Examples of alternative punishments include sentencing an airport handler convicted of theft to clean out the horse stalls at police stables,[146] and broadcasting photographs of people arrested for prostitution offenses on local television.[147] These measures exemplify the alternative punishment notion of "shaming," whereby the offender is forced to "go public" to endure some form of humiliation that imposes accountability for the offensive conduct. The hope is that "shaming sentences, especially those sentences requiring an apology or confession, may fulfill the basic principles of restitution."[148]

---

[144] *Id.* "[T]he seeming paradox of public opinion." (citing J. Doble, *Restorative Justice and Community-Based Reparative Boards: The View of the People of Vermont*, Doble Research Associates, Feb. 1999) (explaining that "[o]n the one hand, the public apparently wants more punishment. On the other hand, the citizenry does not want non-violent offenders in prison, and they favor, sometimes strongly, the use of alternatives to incarceration.").

[145] *Development in Law: Alternatives to Incarceration*, 111 HARV. L. REV. 1863, 1875 (1998) ("Experimentation with alternative punishments must occur now, not only because crimes and criminals are diverse and may require differing treatments, but also because the current demographics of the prison system simply cannot be sustained in the long run.").

[146] *Development in Law: Alternatives to Incarceration*, 111 HARV. L. REV. 1967, 1981 (1998).

[147] *See Development in Law: Alternatives to Incarceration*, *supra* note 145, at 1872 (referring to "John TV" in Kansas City, Missouri where a local government channel broadcasted the photographs and biographical information of persons arrested for offenses related to prostitution).

[148] *See Development in Law: Alternatives to Incarceration*, *supra* note 146, at 1973.

Many opponents of "shaming" criticize its ability to reform criminal behavior[149] and question its functionality; because "degrees of shame are difficult to quantify,"[150] there is no guarantee that the offender experiences true accountability after enduring the alternative punishment. Employing a "shaming" scheme as punishment for circumvention of governmentally-imposed computer monitoring invokes these problems. The restitution principle driving the ideology does not square with a non-violent offense such as software circumvention because there is no tangible "victim" that can benefit from an apology or a confession. One who disables a keystroke monitor to access child pornography commits a wrong to the justice system as a whole by failing to uphold his probationary agreement. However, it is difficult to craft an effective alternative through "shaming" which focuses on the "victim," short of ordering the offender to mop up the local courthouse floors.

Moreover, an offender convicted of possessing child pornography has already suffered the consequence of public humiliation from that crime during his original conviction. Notice to others of his continued indulgence in the egregious behavior via an alternative "shaming" punishment will not likely faze him to the degree necessary to truly punish or prevent future circumvention activity. In fact, the focus on the offender as a pariah is notably diluted after conviction if he circumvents monitoring software, because the humanistic dimension driving society's emotional response to the reprehensible content of the original offense is replaced with a concentration on the illegal technological intricacies involved in the circumvention crime.

Finally, there is no evidence that the threat of public "shaming" would provide any level of reform or serve as a deterrent to make offenders reconsider a potential act of circumvention.[151] Not only does the anonymity of the Internet work to conceal the identity of the user, but it also obscures the identities of the victims. Those who traffic in child pornography are unlikely to actually know or encounter the children in the images they share. Without a personal connection or stake in the activity, these offenders will not feel any sting of punishment that seeks to take advantage of conscience or reputation.

---

[149] *Id.* at 1972.

[150] *Id.* at 1971.

[151] Shaming is most effective when accompanied by restitution to a victim. *See Development in Law: Alternatives to Incarceration*, *supra* note 146, at 1973. But there is arguably no cognizable victim in the context of restricted Internet access for non-violent computer criminals, thus reinforcing the idea that shaming is not an appropriate punishment for this type of probationary violation. *See supra* note 146.

Even if "shaming" were a suitable option for non-violent offenders who violate conditions of probation, those who support alternative punishments comment that federal courts face particular barriers and constraints in employing the measures.[152] These commentators explain that judges are often bound by the system: "[t]he combination of the [Federal Sentencing] Guidelines and the statutorily mandated minimum sentences for many federal crimes does not regularly leave judges the option to experiment with various terms of probation."[153] The Guidelines create four "zones" that determine the baseline range for any sentence, combining an offender's past criminal history with the offense level of the crime committed, as determined by statute, affording judges little discretion to impose alternative punishments beyond first-time non-violent offenses.[154] Furthermore, over one hundred federal laws require mandatory minimum sentences that trump the sentencing ranges in the Guidelines.[155] Thus, judges cannot rely on their discretionary powers alone to craft effective deterrent measures within conditions of probation.

Clearly, alternative punishments designed around "shaming" are inadequate to prevent and punish circumvention of software technology. "Shaming" has been criticized for its inability to reform and its constrained use under the Guidelines. Without an alternative punishment scheme, current consequences provide little deterrence to probation violators because they are unlikely to face prison sentences, reinforcing a credibility gap which extends to non-violent offenders such as computer criminals. A new statute that criminalizes software circumvention and establishes additional civil penalties will fortify the consequences of violating a probationary condition that restricts Internet access after a conviction for trafficking online child pornography.

VII. CREATION OF SEPARATE AND INDEPENDENT CRIMINAL AND CIVIL OFFENSES IS THE PROPER PUNISHMENT SOLUTION

The creation of separate and independent criminal and civil offenses is an effective solution to deter circumvention of probationary restrictions for computer crimes. Statistics are clear that monitoring computer activity alone will not suffice to deter circumvention efforts that overcome restricted Internet access.[156] According to Department of Justice figures, the Federal Bureau of Investigation failed to shut down a proliferation of child pornography websites or web hosts in Fiscal Year

---

[152] *Id.* at 1983.
[153] *Id.*
[154] *Id.* at 1985.
[155] *Id.*
[156] *See infra* note 157.

2006, instead dismantling less than half of its 2,300 target goal.[157] Recent child predator activity on social networking sites such as MySpace demonstrates how Internet content providers arm offenders with more opportunity to pursue illegal sexual activity than ever before.[158] The expanding costs of re-training probation officers to comply with conditions of supervised release that involve Internet monitoring further the need to supplement such measures with enhanced statutory penalties for software circumvention.

While the Sentencing Reform Act clearly prohibits a defendant from committing an additional federal, state, or local crime,[159] judicial interpretation holds that a probation officer's petition for revocation of supervised release must specify a clear statutory provision for the alleged violation.[160] The lack of existing statutory penalties for circumventing computer technology undermines the purpose of a restrictive probationary condition, since probation officers cannot utilize the violation as leverage to control the offender's computer habits. The typical penalty for a clear violation of a statute is often a return to prison to serve out the remainder of a sentence.[161] Consequently, the creation of statutory criminal and civil penalties that target circumvention of computer monitoring technology would significantly bolster the deterrent power of probation by arming it with an effective threat of strict liability incarceration.

Moreover, child pornography is a toxic issue for juries; it results in unsettling litigation that often involves graphic visual evidence. Any measure that reduces jury exposure to explicit evidence would benefit all participants in the judicial system.[162] Prosecutors and defendants alike

---

[157] Only 906 child pornography websites were shut down in Fiscal Year 2006, according to the United States Department of Justice. *See* FY 2006 Performance and Accountability Report, http://www.usdoj.gov/ag/annualreports/pr2006/P1/p10.pdf (last visited Mar. 31, 2007).

[158] *See*, *e.g.*, Matt Richtel, *MySpace.com Moves to Keep Sex Offenders Off of Its Site*, N.Y. TIMES, Dec. 6, 2006, at C3 (indicating that MySpace.com is "developing technologies that would help combat the use of its site by sexual predators by cross-referencing its more than 130 million users against state databases of registered sex offenders.").

[159] *See* 18 U.S.C. § 3563(a)(1), (3), (6), (7) (2006).

[160] *See* United States v. Chatelain, 360 F.3d 114 (2d Cir. 2004); United States v. Havier, 155 F.3d 1090 (9th Cir. 1998).

[161] Department of Justice statistics demonstrate that only 23% of prisoners incarcerated for probation or parole violations were sent to prison for technical violations. The remaining 77% were incarcerated for committing new crimes while under community supervision. *See* the Office of Justice Programs statistics, *available at* http://www.ojp.usdoj.gov/bjs/pub/ascii/ppvsp91.txt (last visited Sept. 23, 2007).

[162] Mock jurors were more likely to feel emotional distress and reported physical reactions in response to viewing graphic photographs. *See* Kevin S. Douglas, David R.

could rely on the assurance from a bright line strict liability regime that informs a defendant—*at his original sentencing stage*—of the additional consequences that would follow any attempt to circumvent the monitoring technology imposed at sentencing. The gravity of computer crimes involving child pornography sharpens the government's policy interest in punishing child predators, justifying the fortification of probationary conditions through independent statutory penalties against circumvention of software monitoring technologies.

A. The Digital Millennium Copyright Act is an Appropriate Model for a New Statutory Scheme

This comment suggests that the appropriate statutory model for a software circumvention punishment scheme is the Digital Millennium Copyright Act ("DMCA"), which created a new category of copyright law in 1998 criminalizing any producer or distributor of technology that functions to circumvent protected access to copyrighted works.[163] The statute carves out exceptions for lawful investigations and intelligence activities by authorized government officials.[164] Applying the same principle to probationary restrictions on Internet access, any circumvention of surveillance techniques for the law enforcement purpose of enforcing the condition could become an independent cause of action that incurs its own parallel penalties.

1. The Rise of Criminal Copyright Infringement

Traditional copyright law treated infringement as a minor criminal wrong, envisioning a one-year imprisonment term for misdemeanor offenses such as unlawful dramatic and musical performances.[165] However, amendments to the 1909 Copyright Act in 1976 and again in 1982 revamped the criminal provisions to create a felony-class offense for certain types of first-time willful infringing uses.[166] Congress responded to the growth of the Internet and the ease of online infringement in 1997 with its passage of the No Electronic Theft Act, widening the scope of felony criminal copyright infringement to include

---

Lyon & James R. P. Ogloff, *The Impact of Graphic Photographic Evidence on Mock Jurors' Decisions in a Murder Trial: Probative or Prejudicial?*, 21 LAW & HUM. BEHAV. 485, 485 (1997).

[163] 17 U.S.C. § 1201 (2006).

[164] § 1201(e).

[165] Laura Gasaway, *Criminal Copyright Infringement*, INFORMATION OUTLOOK, April 2004, *available at* http://findarticles.com/p/articles/mi_m0FWE/is_4_8/ai_n6108144.

[166] *Id.* (noting that the 1982 amendment classified certain activities as felonies depending on the number of infringing copies made or sold with a 180-day period, and increased penalties up to five years in prison and $250,000 in fines).

a maximum prison term of one-year imprisonment for first-time infringers that were not seeking commercial gain.[167] The criminal treatment of purposeful infringement of copyrighted material for personal as well as commercial use was enhanced in 1998, when Congress enacted the DMCA to provide criminal penalties for activities that lead to infringement.[168]

The act of circumventing technological protection is defined within the DMCA as "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[169] The DMCA refers to technology such as video cassette recorders and computer software.[170] The statute controls access to copyrighted works to prevent infringement, penalizing manufacturers of circumvention technology as well as users, to maximize the threat of infringement liability.[171] Section 1203 provides for civil remedies that include actual damages as well as any additional profits earned by the violator.[172] Provisions allow a complaining party to elect statutory damages for each circumvention violation in a range of $200 through $2,500 "per act of circumvention, device, product, component, offer, or performance of service, as the court considers just."[173] Financial statutory penalties increase within a range of $2,500 through $25,000 for attempts that induce, enable, facilitate, or conceal copyright infringement.[174] The current act builds in seven limited exemptions that allow circumvention of access and copy controls for certain activities such as educational and research tasks.[175] The entirety of section 1201 in the DMCA is known as the anti-circumvention provision. As of May 2007, the Department of Justice introduced a bill that will potentially permit a judge to award damages for each separate piece of a copyrighted work rather than applying the infringement analysis to an entire work or compilation.[176] Consequently, law enforcement officials appear poised to expand these provisions.

---

[167] *Id.*; *see also* 18 U.S.C. § 2319 (2000), which indicates that a commercially motivated infringer may receive a federal prison term of five years and $250,000 in fines, whereas a non-commercial infringer is subject to a one-year prison term and $100,000 in fines. Repeat infringers may receive a ten-year federal prison term for commercially-motivated infringements, and up to six years for noncommercial infringements.

[168] *See* 17 U.S.C. §§ 1201–1205 (2006) (making it a criminal violation to circumvent encryption codes set in place to prevent copying).

[169] § 1201(b)(2)(A).

[170] *See* § 1201(k), 1201(b)(1).

[171] *See* § 1201(b)(1).

[172] 17 U.S.C. § 1203(c)(1)(a) (2006).

[173] § 1203(c)(3)(A).

[174] §§ 1202, 1203(c)(3)(B).

[175] § 1201(d)–(j).

[176] Posting of Derek Slater to Electronic Frontier Foundation, http://www.eff.org/deeplinks/archives/005381.php (July 26, 2007, 16:48 EST) (referring

2. Criminal Sanctions Are Ideal for Violations of Probationary Conditions Based on Restricted Internet Access

The expanded criminal statutory scheme within the DMCA has endured a share of criticism for its danger of chilling creative development of new ideas or products at the expense of forming a social norm against conduct that is not currently viewed as immoral.[177] In practice, initial criticism waged against the DMCA's anti-circumvention provision considered it bad public policy, due to its weak enforcement record[178] and ineffectual application to overseas activity.[179] Criminal law necessarily evolves to respond to changes in technology and society, based on concepts of preventing harm to the community and condemning behavior generally regarded as immoral.[180] Criminalization in the copyright infringement context is not an effective deterrent because scores of people continue to copy while the evolving legal standard selects only a small handful of violators in an unsuccessful attempt to build a shared moral code against infringing activity.[181] Further, a deterrence effort through criminalization is most understandably justified when there is a cognizable harm to the protected person, but when people only infringe for personal use, linking a causal harm to infringement is speculative at best because other factors may account for sales declines, since personal use does not impact market share.[182]

---

to the Intellectual Property Enhanced Criminal Enforcement Act of 2007, H.R. 3155, 110th Cong. (2007)), *available at* http://www.govtrack.us/congress/bill.xpd?bill=h110-3155 (last visited Sept. 15, 2007).

[177] Geraldine Szott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. REV. 731, 774 (2003) (explaining how courts are "generally cautious when deciding whether conduct in which citizens routinely engage [copying copyrighted material for personal use] is a crime.").

[178] Eric Goldman, *'No Electronic Theft Act' Proves a Partial Success*, NAT'L L.J., March 17, 2003, at B9, *available at* http://www.ericgoldman.org/Articles/nljnetact.htm (noting how the limited number of criminal copyright prosecutions to that date—eight in five years—demonstrated the DMCA's weak power of deterrence and unpredictable sentencing).

[179] Laura Gasaway, *Enforcement of DMCA Criminal Penalties Suffers Setback*, INFORMATION OUTLOOK, March 2003, *available at* http://findarticles.com/p/articles/mi_m0FWE/is_3_7/ai_99011612 (discussing United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002), a case that represented the first criminal prosecution under the DMCA's anti-circumvision provision, in which the jury acquitted a Russian computer programmer of all charges, partially because there was no proven intention to violate United States law).

[180] *See Moohr*, *supra* note 177 at 751.

[181] *Id.* at 776 (referencing the "Napster experience" to illustrate the "ineffectiveness of legal prohibitions in forming social norms" while consumers continue to engage in infringing activity such as file sharing).

[182] *Id.* at 753–55.

In contrast, the traditional criminal punishment setting is wholly appropriate for independent statutory civil and criminal penalties that condemn software circumvention efforts. Forming social norms through criminal laws is most compelling when it is based on an existing moral code.[183] Unlike the copyright setting, using criminal sanctions to forge a new community norm is unnecessary in the probationary context, because crime and conviction are openly acknowledged responses to violations of established societal norms; the additional sanctions serve as a complementary deterrent measure to promote understood societal expectations. In addition, the harm to the community can already be characterized as a general threat to public safety and stability when the new (probationary) violation is connected to conduct from a prior criminal conviction, regardless of the nature of the violation itself. The harm falls within the conventional notions of punishment when the perpetrator is an already- convicted offender with clear notice of the conditions he must adhere to within the parameters of the initial probationary sentence.

3. The Application of the DMCA Model is Appropriate for a New Statutory Scheme Aimed at Offenders Who Circumvent Forensic Monitoring Techniques

Applying the underlying principles and statutory scheme from the DMCA, punishment for circumventing forensic monitoring software should be a separate and independent violation of a probationary term. Computers, like the technologies addressed by the DMCA, serve a dual-use function. They are unique tools for research and structuring information, but also carry the potential to perform criminal acts. Congress has the constitutional grant of power to enact a strict liability regime that addresses particular software circumvention techniques by sex offenders whose restricted access to the Internet derives from Federal Sentencing conditions of probation.[184] The government has a compelling interest in preventing crime. It can sidestep any opponents who question congressional regulation of the Internet by arguing that the punitive scheme is not an attempt to control Internet content in general—a proper rebuttal would indicated that the statutory scheme encompasses a narrowly-tailored effort that is deeply-rooted in the sentencing and punishment of specific online sexual offender conduct in particular.[185]

---

[183] *Id.* at 777 (citing various texts that discuss the retributivist theory of criminal punishment and the interplay between community values and the law).

[184] U.S. CONST. art. 1, § 8, cl. 18.

[185] Some policy analysts, such as the Cato Institute, fear a chilling effect from any Federal Communications Commission regulation that attempts to regulate Internet access

In enacting additional penalties for circumvention activity, for example, Congress could copy the civil remedy structure from the DMCA to impose financial obligations on an offender who disables a keystroke detector. Penalties might be levied depending upon the degree of circumvention; for example, one possibility enabling access to child pornography is through a proxy server that bypasses all filtering measures, so the court could impose the highest possible fine or incarceration period for this high-level offense. While courts have struggled to draft and tailor monitoring conditions, a statute with strict liability language would enable courts to impose clear guidelines and penalties across the board for all types and levels of circumvention (for example, the statute may establish one definition of "circumvention" to include using more than one designated computer at the offender's home.) Other definitions of "circumvention" could expand its scope to address particular instances of software circumvention ostensibly committed by the savviest offenders, with delineated bright line civil penalties and mandatory incarceration determined by the nature of the technique the offender used to circumvent the software.

The strict liability attribute of statutory circumvention penalties also provides distinct notice to offenders about the consequences of circumvention, injecting a fortified threat to provide additional deterrence where the gaps in credibility for probationary violations and options of alternative punishments currently fall short. Thus, the DMCA is an excellent model to resolve the software circumvention problem by providing additional civil and criminal sanctions aimed at offenders who circumvent technology imposed as a condition of probation.

VIII. CONCLUSION

The circuit courts of appeals divide when considering the scope of restrictive conditions surrounding Internet access for sex offenders sentenced to probation or supervised release after a conviction for online trafficking of child pornography. The Second and Eighth Circuits have reversed Internet restrictions on the ground that such conditions were overbroad in the context of the defendant's Fourth Amendment rights. In contrast, the Ninth and Eleventh Circuits acknowledged that careful tailoring of the language in the condition and careful selection of the enforcement technology can combine to render restrictive Internet conditions an entirely appropriate punishment.

---

and content. *See, e.g.*, Thomas W. Hazlett & David W. Sosa, *Chilling the Internet? Lessons from FCC Regulation of Radio Broadcasting*, CATO POLICY ANALYSIS NO. 270, Mar. 19, 1997, http://www.cato.org/pubs/pas/pa-270.html (last visited Sept. 30, 2007).

Supreme Court jurisprudence suggests that status as a probationer or parolee reduces that person's Fourth Amendment rights, permitting the inference that a partial or total ban on Internet access does not infringe on the privacy rights of convicted sex offenders. However, enforcing such restrictive conditions on Internet access is impractical and burdensome, due to the impracticalities of curbing offender exposure to the Internet in modern society. Further, there are prohibitive costs when training officers to track the offenders' computer activities using forensic software, filtering, and monitoring technology.

The credibility crisis in the probationary punishment scheme weakens the current deterrent value of restrictive conditions against sex offenders subjected to forensic monitoring or filtering of their Internet activities. Moreover, statistics highlight the failure of punishment for probationary violations as a viable threat against non-violent offenders. In addition, an alternative punishment scheme is not appropriate for probationers convicted of trafficking online child pornography because its capacity to "shame" the defendant is likely to be diluted and ineffective.

Courts often employ legal balancing tests that weigh the totality of circumstances in each particular lawsuit,[186] but bright line rules offer a certainty of consequence that benefits all participants in the justice system. Clearly, punishment solely by the terms of probation is not adequate. Enacting additional and independent criminal and civil offenses premised on strict liability for any probationer activity that circumvents the government's efforts to make safe dual-use technologies following a conviction for viewing, possessing, or distributing online child pornography will clarify litigation and give notice to defendants that restrictions on Internet use are serious measures that warrant compliance. The deterrent value in such a solution will ensure that the criminal justice system regains the respect of the public and offender alike, to prevent any further exploitation of children.

---

[186] Two examples of Totality of the Circumstances tests that evaluate factors under the Fourth Amendment include determining whether there was probable cause preceding a search and whether police questioning created an unreasonable atmosphere of coercion.