DEPUTIZING INTERNET SERVICE PROVIDERS: HOW THE GOVERNMENT AVOIDS FOURTH AMENDMENT PROTECTIONS

*ALEXANDRA L. MITTER**

INTRODUCTION

Not until the late 1970s did law enforcement in the United States begin to recognize and address the existence of child pornography.[1] The response was quick and efficient, and over the ensuing four decades, an admirable alliance of federal and state law enforcement has made great strides in eliminating the presence and trafficking of child pornography in the United States. Unfortunately, the rise of the Internet has complicated these law enforcement efforts, providing a new avenue for pedophiles[2] and traffickers to access and trade images in relative anonymity. The Internet's effect on child pornography has provoked an equally swift response, leading to the enactment of several statutes that pro-

* J.D., New York University School of Law, 2011.

1. *See* Amy Adler, *The Perverse Law of Child Pornography*, 101 COLUM. L. REV. 209, 219–34 (2001) (noting a dramatic rise in the reported instances of child abuse and highlighting the potential causes: increased incidences, increase in awareness, better reporting, expanded definitions); JOEL BEST, THREATENED CHILDREN: RHETORIC AND CONCERN ABOUT CHILD-VICTIMS 171 (1990). The discovery of "battered-child syndrome" in 1962 led to a flurry of child abuse literature, but not until later did the sexual abuse of children supersede violent abuse in importance in the public consciousness. *See generally* Ian Hacking, *The Making and Molding of Child Abuse*, 17 CRITICAL INQUIRY 253 (1991).

2. The American Psychiatry Association's Diagnostic and Statistical Manual IV includes "pedophilia" in its list of sexual and gender identity disorders. Pedophilia is marked by "recurrent, intense sexually arousing fantasies, sexual urges, or behaviors involving sexual activity with a prepubescent child or children (generally age 13 years or younger)." AMERICAN PSYCHIATRIC ASS'N, DIAGNOSTIC AND STATISTICAL MANUAL OF MENTAL DISORDERS 571–72 (4th ed. 2000). The proposed revisions to the Diagnostic and Statistical Manual do not substantively change the characteristics of the disorder. The APA proposes to change the disorder's name from "pedophilia" to "pedohebephilic disorder" and increase the maximum age from 13 to 14. The APA estimates that little to no increase in the number of diagnoses will occur because of the new definition. *See* AMERICAN PSYCHIATRIC ASS'N, DIAGNOSTIC AND STATISTICAL MANUAL OF MENTAL DISORDERS 302.2 (proposed revisions), *available at* http://www.dsm5.org/ProposedRevisions/Pages/proposedrevision.aspx?rid=186.

vide broad investigative and enforcement powers to local and federal law enforcement.[3] However, in attempting to address the proliferation of child pornography on the Internet, Congress and law enforcement agencies have created enormous Fourth Amendment issues for all Internet users. The facilitation of widespread Internet Service Provider (ISP) monitoring programs jeopardizes the rights of all Internet users to be free from unreasonable intrusion.

While the Internet's position in Fourth Amendment jurisprudence has received extensive scholarly attention, the investigation of child pornography on the Internet has not.[4] This is due in part to the lack of a statutory remedy for law enforcement violations of the governing legislation, the Stored Communications Act (the SCA). By explicitly not including a suppression remedy, the Stored Communications Act provides little incentive for a defendant to make a Fourth Amendment challenge.[5] Consequently, the Stored Communications Act has not been subject to the rigorous judicial analysis that it deserves, leaving the "famously complex"[6] law of electronic surveillance without elucidation.[7] This lack of relevant case law in turn contributes to the dearth of academic attention on the interaction of the SCA and the Fourth Amendment.

This Note seeks to address this academic and jurisprudential gap.[8] Its argument is two-fold: first, it explains why private Internet

3. *See, e.g.*, Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, 102 Stat. 4485 (codified as amended at 18 U.S.C. § 2251 (2006)); Child Pornography Prevention Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009 (codified in scattered sections of Titles 18 and 42 U.S.C.); PROTECT Act of 2003, Pub. L. No. 108-21, 117 Stat. 650, 676–86 (codified in scattered sections of Title 18 U.S.C.).

4. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Ric Simmons, *From* Katz *to* Kyllo: *A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technology*, 53 HASTINGS L.J. 1303 (2002); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011).

5. 18 U.S.C. § 2708.

6. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003).

7. *See id.* at 807; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1277 (2004).Though largely beyond the scope of this Note, both Professor Kerr and Professor Solove's articles provide an interesting argument in favor of including a suppression remedy in internet surveillance laws.

8. *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010) (noting that the jurisprudence and legal scholarship are sparse on the application of the Fourth Amendment to the internet context); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008), *rev'd*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) ("The recently

activity should always be protected by the warrant and probable cause requirements of the Fourth Amendment; second, it contends that, through statutory enactments and local law enforcement action, ISPs are turned into agents of law enforcement, which should cause their private monitoring programs to trigger Fourth Amendment protections.

In making this argument, the Note will proceed in five parts. Part I traces the rise in awareness of child pornography in the United States and the Internet's unique role in the proliferation of child pornography. Part II analyzes the statutes currently protecting Internet activity, with a special emphasis on the provisions regulating child pornography on the Internet. Part III provides an outline of Fourth Amendment jurisprudence and situates Internet monitoring within it, arguing that private Internet activity merits the protection afforded by the requirement of a warrant supported by probable cause. Part IV then addresses common counterarguments for keeping Internet monitoring outside the scope of the Fourth Amendment. Finally, Part V argues that congressional statutes and state law enforcement agents have deputized ISPs through subtle encouragement and coercion.

I.
CHILD PORNOGRAPHY LAW AND THE INTERNET

Child pornography, as a separately criminalized and distinct phenomenon from pornography featuring adults, is relatively new.[9] Despite its rampant availability, child pornography did not provoke a widespread moralistic response until the late 1970s.[10] However, once discovered and recognized as a unique problem, child pornography was swiftly dealt with through an alliance of federal law enforcement agencies. According to the Child Exploitation and Obscenity Section of the United States Department of Justice, by the 1980s, law enforcement had virtually eliminated the problem of child pornography trafficking.[11] With the advent of the Internet,

minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.").

9. *See, e.g.*, New York v. Ferber, 458 U.S. 747 (1982) (holding that unlike adult pornography, child pornography is not entitled to First Amendment protection).

10. PHILIP JENKINS, BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET 32–33 (2001).

11. U. S. DEP'T OF JUSTICE, CHILD EXPLOITATION AND OBSCENITY SECTION, http://www.justice.gov/criminal/ceos/childporn.html (last visited April. 18 2011) [hereinafter DOJ CHILD EXPLOITATION]; *see also* ATT'Y GEN.'S COMMISSION ON POR-

however, child pornography has reappeared in a more pervasive and virulent form.[12] The Internet has increased the amount of material available to users and drastically improved distribution and accessibility.[13] Now, a single image reproduced on the Internet may be accessed by an increasingly large number of anonymous individuals around the globe.

This Section traces the rise in awareness of child pornography and the federal government's response to this new problem, leaving a more complete discussion of the current law for later in the Note.[14] This Section will then discuss the role of the Internet in shaping the current child pornography landscape and legislation.

A. The "Discovery" of Child Pornography and Legal Response

In 1986, the United States Office of the Attorney General's Commission published a report on pornography.[15] The Commission's discussion of child pornography is premised on a conception of each image as an individual instance of sexual exploitation.[16] This understanding of child pornography placed it within a larger hysteria surrounding child abuse that began in the 1970s.[17] The problem of child pornography, independent from concerns about adult pornography, could not surface until the media (and, subsequently, law enforcement) raised public awareness about the specter of child abuse.[18] While estimates of the prevalence of child pornography at that time varied greatly, rooting out child

NOGRAPHY, FINAL REPORT 408–09 (1986), *available at* http://porn-report.com/contents.htm [hereinafter ATTORNEY GENERAL'S REPORT].

12. DOJ CHILD EXPLOITATION, *supra* note 11.

13. *See, e.g.*, William R. Graham, Jr., *Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland,'* 2000 L. REV. M.S.U.-D.C.L. 457, 465 (2000) (discussing how the internet enables rapid transfer of files and images, provides relatively high security, and almost complete anonymity for its users); RICHARD WORTLEY & STEPHEN SMALLBONE, U.S. DEP'T OF JUSTICE, OFFICE OF CMTY. ORIENTED POLICING SERVS., CHILD PORNOGRAPHY ON THE INTERNET PROBLEM-ORIENTED GUIDES FOR POLICE, PROBLEM-SPECIFIC GUIDES SERIES NO. 41, 8 (2006) [hereinafter COPS GUIDE] ("The Internet has escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution, and the ease of its accessibility.").

14. *See infra* Parts II–III.

15. ATTORNEY GENERAL'S REPORT, *supra* note 11.

16. *Id.* at 405–6.

17. For a detailed discussion of the discovery of child abuse and child pornography's role within it, see Adler, *supra* note 1, at 214–34.

18. *Id.* at 219–21.

pornographers and pedophiles became an issue at the forefront of law enforcement concerns.[19]

Major legislative and law enforcement efforts began in the late 1970s in response to the growing concern about the proliferation of child abuse and child pornography.[20] Congress passed the Protection of Children Against Sexual Exploitation Act in 1978, criminalizing the use of children in the production of obscene images.[21] Not until *New York v. Ferber*,[22] however, did the Supreme Court recognize child pornography as a category of pornographic material unprotected by the First Amendment for reasons independent of the image's obscenity. By eliminating the requirement that the image fall within the definition of "obscene" established in *California v. Miller*,[23] *Ferber* exposed child pornography to a host of new federal and state regulations. After *Ferber*, virtually every state added sanctions to its criminal law for the production, promotion, sale, distribution, or exhibition of pornographic images involving chil-

19. The Attorney General's 1986 report noted that between January 1, 1978 and February 27, 1986, 255 individuals were prosecuted under federal child pornography statutes. However, the Attorney General estimated that this was an underrepresentation because before 1982 the definition of child pornography still included the obscenity requirement. ATTORNEY GENERAL'S REPORT, *supra* note 11, at 415–16. More recent estimates indicate that there are "more than one million pornographic images of children on the Internet, with 200 new images posted daily." COPS GUIDE, *supra* note 13, at 12. *See also* JENKINS, *supra* note 10, at 33; Khalid Khan, *Child Pornography on the Internet*, 73 POLICE J. 7, 9–10 (2000). The number of child pornography prosecutions has dramatically increased as well, peaking in 2006 with more than 1,500 cases. *Pornography—Child Prosecutions for 2010*, TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, http://tracfed.syr.edu/results/9x204db7748fc1.html (last accessed April 25, 2011). Despite attempts to quantify the prevalence of child pornography on the Internet, there is recognized difficulty in making a complete and accurate assessment. *See* EVA J. KLAIN, HEATHER J. DAVIES & MOLLY A. HICKS, AM. BAR ASS'N CTR. ON CHILDREN & THE LAW, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, CHILD PORNOGRAPHY: THE CRIMINAL-JUSTICE-SYSTEM RESPONSE 3 (2001) ("Accurate estimates are difficult because no valid and reliable methodology has been devised to measure the amount of child pornography especially on the Internet.").

20. ATTORNEY GENERAL'S REPORT, *supra* note 11, at 408.

21. Protection of Children Against Sexual Exploitation Act of 1978, Pub. L. No. 95-225, 92 Stat. 7 (1978) (codified as amended at 18 U.S.C. §§ 2251–2253 (2006)).

22. 458 U.S. 747, 774 (1982).

23. 413 U.S. 15, 25 (1973) (setting forth a three-part test for obscenity: (1) contemporary community standards must find that the work as a whole appeals to "prurient interests"; (2) the work must depict sexual conduct in a patently offensive way and; (3) the work must lack serious literary, artistic, political, or scientific value).

dren.[24] Congress responded to *Ferber* by passing the Child Protection Act of 1984, which expanded the reach of federal criminal law to cover non-obscene images of children.[25]

In 1996, Congress once again expanded the reach of child pornography regulation through the Child Pornography Prevention Act (CPPA).[26] The CPPA criminalized "virtual" child pornography by including within its definition of child pornography any image that has been modified or generated by computer to appear to be of a minor engaging in sexual conduct.[27] The Supreme Court, in *Ashcroft v. Free Speech Coalition*,[28] struck this provision as a violation of the First Amendment, rejecting the argument put forward in *Ferber* that child pornography is "'intrinsically related' to the sexual abuse of children."[29] Absent harm to an actual child, virtual child pornography would receive First Amendment protection. In response to the Supreme Court's decision, Congress enacted the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (the PROTECT Act), the primary tool by which the federal government defines and regulates the production and distribution of child pornography today.[30] The PROTECT Act criminalizes the knowing production, distribution, receipt, or possession of images determined to constitute child pornography.[31]

The PROTECT Act addressed the Supreme Court's concerns in *Ashcroft v. Free Speech Coalition* by defining child pornography as a "visual depiction of any kind, including a drawing, cartoon, sculpture or painting" depicting "a minor engaging in sexually explicit conduct" that "is obscene," or "depicts an image that is, or appears to be, of a minor engaging in . . . sexual intercourse . . . and lacks serious literary, artistic, political, or scientific value."[32] While it maintained the definition of actual, not virtual, child pornography, it brought virtual images falling under the *Miller* definition of "ob-

24. ATTORNEY GENERAL'S REPORT, *supra* note 12 at 415.

25. Child Protection Act of 1984, Pub. L. No. 98-292, 98 Stat. 204 (codified as amended at 18 U.S.C. §§ 2251–2254, 2256, 2516 (2006)).

26. Child Pornography Prevention Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009 (codified in scattered sections of Titles 18 and 42 U.S.C.).

27. Child Pornography Prevention Act of 1996, 18 U.S.C. § 2256(8)(B)–(C) (2006).

28. 535 U.S. 234 (2002).

29. 535 U.S. at 250 (quoting United States v. Ferber, 458 U.S. 747, 759 (1982)).

30. PROTECT Act of 2003, Pub. L. No. 108-021, 117 Stat. 650 (2003).

31. PROTECT Act of 2003, 18 U.S.C. § 1446A(a)–(b) (2006).

32. *Id.*

scene" back into its purview.[33] Similarly, the PROTECT Act criminalizes the knowing advertisement or distribution of "an obscene visual depiction of a minor engaging in sexually explicit conduct; or a visual depiction of an actual minor engaging in sexually explicit conduct."[34] Additionally, pandering or soliciting material purported to contain such a depiction is a violation even if the actual material does not meet the statute's definition.[35]

The current law creates a mandatory minimum sentence of five years for first time offenders, with discretionary sentences of up to twenty. Repeat offenders can receive sentences ranging from fifteen to forty years.[36]

B. The Internet and the Proliferation of Child Pornography

Before the advent of the Internet, production and reproduction of pornographic images involving children were extremely difficult and expensive, and the sale and distribution of those images were similarly risky endeavors.[37] Child pornographers, producing and dealing in hard copies, were traceable individuals. However, as the Attorney General's Report notes, by 1986 child pornographers were beginning to use computer networks in addition to the mails to exchange photographs.[38] The Attorney General's Commission suggested legislation addressing the use of new technologies, specifically computers, in the production and distribution of child pornography.[39] Today, "[t]he technological ease, lack of expense, and anonymity in obtaining and distributing child pornography has resulted in an explosion in the availability, accessibility, and volume

33. The history of the application of obscenity doctrine to pornographic images is one fraught with difficulty for the Supreme Court and has been often criticized by academics, but obscenity prosecutions have experienced a resurgence after the Court's decision in *Ashcroft*. *See* Amy Adler, *All Porn All the Time*, 31 N.Y.U. REV. L. & SOC. CHANGE 695, 704–10 (2007).

34. 18 U.S.C. § 2252A(a)(3)(B)(i)–(ii) (2006).

35. *Id.* Although *Ashcroft v. Free Speech Coalition* struck down a provision classifying as child pornography all material that "conveys the impression that it depicts a minor engaging in sexually explicit conduct," 535 U.S. 234, 257–58 (2002), the Court upheld the PROTECT Act's narrower pandering-and-solicitation provision. United States v. Williams, 553 U.S. 285, 286 (2008) ("The constitutional defect in *Free Speech Coalition*'s pandering provision was that it went beyond pandering to prohibit possessing material that could not otherwise be proscribed.").

36. 18 U.S.C. § 2252A(b)(1) (2006).

37. DOJ CHILD EXPLOITATION, *supra* note 12; *see also* JENKINS, *supra* note 11, at 52–58.

38. ATTORNEY GENERAL'S REPORT, *supra* note 12, at 407.

39. *Id.* at 443.

of child pornography."[40] The Department of Justice, having determined that it has virtually eradicated the domestic distribution of child pornography in hard copy, now focuses its efforts on a similar eradication of online materials.[41]

The federal statutory law has largely kept pace with technological advancements,[42] although some have argued that congressional lag time is too long.[43] In 1988 Congress passed the Child Protection and Obscenity Enforcement Act, which for the first time made it illegal to use a computer to depict or advertise child pornography.[44] The current law, the PROTECT Act, also includes computers in every discussion of mailing, transporting, or distributing child pornography through interstate and foreign commerce.[45] Similarly, "visual depiction" includes "data stored on a computer disk or by electronic means[,] . . . digital image or picture, computer image or picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means."[46]

Law enforcement is also exploring new avenues for policing the production and distribution of child pornography on the Internet.[47] The Department of Justice's Office of Community Oriented Policing Services published a guide to Internet child pornography for local law enforcement discussing the various means by which the Internet facilitates child pornography (e-mail, peer-to-peer networks,[48] private message boards) and problems

40. DOJ CHILD EXPLOITATION, *supra* note 11.

41. *Id.*

42. *See, e.g.*, 18 U.S.C. § 2256(8)(C) (including as child pornography visual depictions that have been "created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct"). This section "prohibits a more common and lower tech means of creating virtual images, known as computer morphing. Rather than creating original images, pornographers can alter innocent pictures of real children so that the children appear to be engaged in sexual activity." Ashcroft v. Free Speech Coal., 535 U.S. 234, 242 (2002).

43. *See, e.g.*, Daniel Solove, Professor, George Washington Univ. Law Sch., Privacy v. Security: Has Fourth Amendment Law Kept up with Current Technology?, Address at the N.Y.U. Hoffinger Criminal Justice Colloquium (Nov. 16, 2009); *see also* United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting) (noting that the majority's reliance on *United States v. Knotts*, 460 U.S. 276 (1983), is misplaced given the advancement in GPS technology).

44. Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, 102 Stat. 4485 (codified as amended at 18 U.S.C. § 2252 (2006)).

45. *See* 18 U.S.C. § 1446A(d) (2006); 18 U.S.C. § 2252A(a) (2006).

46. 18 U.S.C. § 1446A(f)(1).

47. *See, e.g.*, COPS GUIDE, *supra* note 13.

48. Peer-to-peer networks are composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coor-

uniquely associated with the investigation of Internet crime (encryption, lack of Internet regulation, volume of Internet activity, jurisdictional questions).[49]

While the need to police child pornography is well recognized by politicians and law enforcement agencies, Fourth Amendment concerns remain: how should these efforts be carried out, and to what extent should ISPs be involved in investigative and regulatory efforts? The remainder of this Note will analyze the statutory framework for regulating and investigating child pornography on the Internet, focusing on Fourth Amendment jurisprudence.

II.
STATUTORY REPORTING REQUIREMENTS FOR INTERNET SERVICE PROVIDERS

The Electronic Communications Privacy Act (ECPA) is the primary statute through which Congress regulates and protects the privacy of Internet activity.[50] It consists of three parts, each of which addresses a particular area of technology: the Wiretap Act,[51] the Pen Register Act,[52] and the Stored Communications Act.[53] The ECPA trilogy is Congress's attempt to protect users of the telephone and Internet from invasions of privacy by service providers, law enforcement officers, and third-party hackers.[54] However, these statutes contain several carve-outs in which a user's activity goes unprotected.

The SCA, passed in 1986, reflected Congress's recognition that the Wiretap Act alone would not provide sufficient protection to the growing group of computer users.[55] The Wiretap Act only protects the communications while they are in transit; information stored on servers used by either the sender or receiver remain un-

dination instances (such as servers or stable hosts). Rüdiger Schollmeier, *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*, 2001 PROC. OF THE FIRST INT'L CONF. ON PEER-TO-PEER COMPUTING 101.

49. *See* COPS GUIDE, *supra* note 14.

50. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

51. 18 U.S.C. §§ 2510–2522 (2006).

52. 18 U.S.C. §§ 3121–3127 (2006).

53. 18 U.S.C. §§ 2701–2712 (2006).

54. *See* S. REP. No. 99-541, at 1–3 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555–58.

55. *See* Solove, *supra* note 8, at 1277 ("[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.") (alteration in original) (quoting H.R. REP. NO. 99-647, at 18 (1986)).

protected. The SCA makes it a crime to intentionally access servers storing electronic communications to obtain, alter, or prevent access to said electronic communication.[56] While generally law enforcement officers are required to procure a search warrant supported by probable cause prior to a search, the SCA creates a bifurcated procedure in which information stored for more than 180 days is treated differently from information stored for less time.[57] For information stored for fewer than 180 days, a warrant is required; however, if the information has been stored for more than 180 days, a warrant may be executed without notice.[58] An administrative subpoena, which requires less than probable cause, or court order executed with notice are also sufficient under the SCA for information stored for longer than 180 days.[59] At any time, and without a warrant, law enforcement may request that an ISP turn over subscriber information, including name, address, local and long distance telephone connection records, and records of session times and durations, length of service and types of service utilized, and means and source of payment for such service, including any credit card or bank account numbers of a subscriber.[60]

This Note argues that the SCA and the PROTECT Our Children Act of 2008[61] combine to create a reporting framework that facilitates the deputization of ISPs and violates the Fourth Amendment rights of every Internet user. The SCA allows an ISP to voluntarily turn over contents of a communication to the National Center for Missing and Exploited Children (NCMEC), a private, non-profit organization founded by Congress in 1984, in conjunction with a report submitted regarding anything under § 2258A—the PROTECT Our Children Act.[62] Under the PROTECT Our Children Act, passed in 2008, any ISP that obtains actual knowledge of child pornography or related offenses is required to make a report to NCMEC's CyberTipline.[63] Failure to report triggers fines of up to $150,000 for the first offense and $300,000 for subsequent viola-

56. 18 U.S.C. § 2701(a).

57. This bifurcation reflects an outmoded understanding of stored electronic communications in which communications left on a server for more than 180 days were considered abandoned for Fourth Amendment purposes. *See* Kerr, *supra* note 4, at 1234.

58. 18 U.S.C. § 2703(a).

59. *Id.* § 2703(b)(1)(B)(i)–(ii).

60. *Id.* § 2703(c)(2).

61. Pub. L. No. 110-401, 122 Stat. 4229 (2008) (codified as amended in scattered sections of 18 U.S.C.).

62. 18 U.S.C. § 2702(b)(6).

63. *Id.*. § 2258A(a).

tions.[64] Though there is no duty to affirmatively seek out this information,[65] in order to facilitate discovery, NCMEC may furnish ISPs with "elements relating to any apparent child pornography image" including "hash values or other unique identifiers."[66]

As mentioned above, the lack of an exclusionary remedy under the SCA has led to a dearth of litigation challenging searches carried out by law enforcement or ISPs pursuant to the exceptions provided in the SCA and PROTECT Our Children Act.[67] However, a lack of challenges should not be interpreted as approval of the searches currently authorized by the statutes. Fourth Amendment challenges can and should be brought by those whose private Internet activities were monitored and exposed by an ISP working in conjunction with federal law enforcement.

III.
FOURTH AMENDMENT JURISPRUDENCE AND THE INTERNET

This section provides an outline of the Fourth Amendment framework and seeks to situate ISP monitoring and statutory reporting requirements in this established jurisprudence. The Fourth Amendment protects "persons, houses, papers, and effects, against unreasonable searches and seizures" and declares that "no Warrants shall issue, but upon probable cause."[68] The issues courts have faced since 1791 are, first, how to define "unreasonable" and, second, the tension between the reasonableness and warrant clauses. The requirement of a warrant supported by probable cause inserts a neutral magistrate between the "zealous officer" and his target.[69] While the general rule is that searches performed without a warrant supported by probable cause are per se unreasonable,[70] over time,

64. *Id.* § 2258A(e).

65. *Id.* § 2258A(f).

66. *Id.* § 2258C(a)(1)–(2). "Hashing is the process of taking an input data string (the bits on a hard drive, for example), and using a mathematical function to generate a (usually smaller) output string." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. 38, 39 (2005).

67. *See supra* note 7 and accompanying text.

68. U.S. CONST. amend. IV.

69. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948) (Fourth Amendment "protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

70. *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 390 (1978).

the Court has carved out exceptions.[71] The touchstone of Fourth Amendment jurisprudence is the courts' assessment of a search and seizure's reasonableness.[72]

The Supreme Court has held that some law enforcement actions do not constitute a "search" within the meaning of the Fourth Amendment.[73] Functionally, the Court breaks Fourth Amendment searches into three discrete categories, each with its own requirements and regulations. First, there are those searches that require law enforcement to obtain a warrant supported by probable cause.[74] Second, some searches may be carried out without a warrant, but require the law enforcement officer to articulate a reasonable suspicion and conduct his search narrowly based on the scope of his or her suspicion.[75] Finally, there are those situations in which law enforcement may search with neither a warrant nor any particularized suspicion.[76]

The Supreme Court has often struggled to fit rapidly changing technologies into this framework.[77] The Court often tries to develop unique tests that will allow the Fourth Amendment to keep pace with technological change.[78] At other times, new developments arrive through congressional statute, as in the case of the ECPA.[79] Through the ECPA, Congress expanded the protections afforded private Internet activity; however, the statute creates sev-

71. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398 (2006) (assisting injured persons); Illinois v. McArthur, 531 U.S. 326 (2001) (destruction of evidence); United States v. Santana, 427 U.S. 38 (1976) (hot pursuit); Chimel v. California, 395 U.S. 752 (1969) (search incident to arrest).

72. Samson v. California, 547 U.S. 843, 855 n.4 (2006).

73. *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983) (a beeper device placed in a car will not constitute a search if police could have followed the car unaided by the technology); United States v. Place, 462 U.S. 696, 697–98 (1983) (use of a narcotics-detecting dog will not constitute a search because only the presence or absence of contraband can be detected and there is no reasonable expectation of privacy in the possession of contraband).

74. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967); Kyllo v. United States, 533 U.S. 27 (2001).

75. *See* Terry v. Ohio, 392 U.S. 1, 19 (1968).

76. *See, e.g.*, Indianapolis v. Edmond, 531 U.S. 32, 37 (2000); Samson, 547 U.S. at 857.

77. *See, e.g.*, *Kyllo*, 533 U.S. 27 (majority and dissenting opinions disagreeing on the implications of new thermal imaging technology).

78. *Id.* at 40 (Courts "must take the long view, from the original meaning of the Fourth Amendment forward."); *see also* United States v. Karo, 468 U.S. 705, 713 (1984).

79. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

eral gaps allowing governmental and private intrusion.[80] This section argues that, because of the Internet's ubiquitous place in society, private Internet activity merits the highest level of Fourth Amendment protection.

A. The Warrant and Probable Cause Requirement

Though the Court often writes of the warrant requirement as the primary protection provided by the Fourth Amendment, new exceptions are continually carved out of the so-called default.[81] The Supreme Court has repeatedly designated the home a bastion of personal privacy requiring the utmost Fourth Amendment protection while leaving other areas of activity as deeply personal as those that take place in the home unprotected by the warrant requirement.[82] Newly developed technologies pose special problems for the courts determining whether and to what extent their uses should be protected.

Initially, the Court's Fourth Amendment jurisprudence drew heavily on property conceptions of privacy, dividing the world into those physical spaces protected by the Amendment and those left unprotected.[83] However, in *Katz v. United States*,[84] the Court rejected the dichotomy of constitutionally protected areas versus unprotected areas, choosing instead to adopt a more nuanced understanding of the privacy protected by the Fourth Amendment, one particularly relevant in governing the protection of new technologies. Justice Stewart, writing for the majority in *Katz*, explained,

80. *See supra* notes 50–60 and accompanying text.

81. *See* Kerr, *supra* note 8, at 1040 n.139–41 (noting the same and citing to Thompson v. Louisiana, 469 U.S. 17, 20 (1984) (per curiam) ("[W]e have consistently reaffirmed our understanding that in all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate between the police and the 'persons, houses, papers, and effects' of citizens.")); Groh v. Ramirez, 540 U.S. 551, 572–73 (2004) (Thomas, J., dissenting) ("[O]ur cases stand for the illuminating proposition that warrantless searches are *per se* unreasonable, except, of course, when they are not.")).

82. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1127 (Reinhardt, J., dissenting) ("These decisions have curtailed the 'right of the people to be secure . . . against unreasonable searches and seizures' not only in our homes and surrounding curtilage, but also in our vehicles, computers, telephones, and bodies—all the way down to our bodily fluids and DNA.").

83. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928) (wiretapping is not a Fourth Amendment violation as there is no physical search or seizure of tangible property); Boyd v. United States, 116 U.S. 616, 622 (1886) (compulsory production of personal property constituted a seizure under the Fourth Amendment unless the property was illegal or stolen).

84. 389 U.S. 347 (1967).

the "Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[85] Justice Harlan's concurrence provides the guiding principle to the present day: if a person has a subjective expectation of privacy and it is one that society is willing to recognize as reasonable, a warrant supported by probable cause will be required to search or seize anything covered by the expectation.[86]

While the Court relies heavily on the "reasonable expectation of privacy" language, many academics assert that it really masks "a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment."[87] The Court has recognized that "no single factor invariably will be determinative" of reasonableness.[88] Even so, it is useful to explore the ways in which Internet users express their subjective expectations of privacy in their online activity and how society buttresses the expectations' reasonableness. A court's assessment of reasonableness—whether normative or descriptive—is crucial because police activity that invades a person's unreasonable expectation of privacy will not constitute a search at all.[89] Electronic communications carried out over the Internet have reached an extraordinary level of importance in day-to-day interactions.[90] Everything from business transactions to medical records and love notes travel through the Internet. People would not be as inclined to extensively use the Internet to communicate if they did not have a subjective expectation that these communications would remain private. The knowledge that an ISP could monitor and read the contents of e-mail correspon-

85. *Id.* at 351–52 (citation omitted).

86. *Id.* at 361 (Harlan, J., concurring).

87. *See, e.g.*, Kerr, *supra* note 8, at 1037–38. *See also* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106–07 (2008) (noting the circularity of the rule's application).

88. Rakas v. Illinois, 439 U.S. 128, 152 (1978) (Powell, J., concurring).

89. *See* Kyllo v. United States, 533 U.S. 27, 32–33 (2001).

90. Data Memorandum from John B. Horrigan, Assoc. Dir., Pew Internet & Am. Life Project, Use of Cloud Computing Applications and Services (Sept. 2008), at 1, *available at* http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf ("Some 69% of online Americans use webmail services, store data online, or use software programs such as word processing applications whose functionality is located on the web.").

dence might chill the widespread use of the Internet.[91] The fact that an ISP has the ability to access online correspondence is not dispositive; a person loses a reasonable expectation of privacy in information accessed by a third party or its employees only "in the ordinary course of business."[92] Society seems to recognize the expectation of privacy in online activity as a reasonable one.[93] By requiring a warrant for police to access e-mails stored for fewer than 180 days, the SCA lends congressional support to the idea that there is a reasonable expectation of privacy in lawful Internet activity.[94] Congress, recognizing that the courts are often slow to protect the use of new technology, saw fit to provide additional statutory protections to electronic communications in order to comport with the public's reasonable expectation that these communications will be protected.[95]

However, the mere presence of statutory protection does not mean that the courts always assume the protection it provides is sufficient; rather, they pay keen attention to the areas in which the statute may fail to provide adequate protection.[96] In her concurrence in *Florida v. Riley*, Justice O'Connor explained that compliance with regulations is not necessarily sufficient to determine whether a reasonable expectation of privacy exists; rather, the Court should determine whether the means by which the intrusion occurred "is a sufficiently routine part of modern life" such that it would be unreasonable for a person not to expect it.[97] The Supreme Court has also assessed the reasonableness of a person's expectation based on the type of technique or technology used in the

91. S. REP. NO. 99-541, at 5, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (noting that lag time in judicial developments "may unnecessarily discourage potential customers from using innovative communications systems").

92. United States v. Miller, 425 U.S. 435, 442 (1976).

93. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.").

94. 18 U.S.C. § 2703(a).

95. Shubert v. Metrophone, Inc., 898 F.2d 401, 404 (3d Cir. 1990) (citing H.R. REP. NO. 99-647, at 18 (1986)) (The "legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology."); *see also* S. REP. NO. 99-541, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens.").

96. Indeed, Orin Kerr argues that 18 U.S.C. § 2703(b) of the Stored Communications Act is unconstitutional. *See* Kerr, *supra* note 8, at 1043.

97. Florida v. Riley, 488 U.S. 445, 453 (1989) (O'Connnor, J., concurring).

intrusion.[98] Where the technology employed is widely available and commonly used, the Court has found that a person's subjective expectations of privacy are less likely to be reasonable.[99]

When determining what protections to afford users of a new technology, analogizing the purposes and functions of the new technology to those of older technologies often provides the most satisfying answer. The telephone presents a useful comparison to Internet communications and e-mail: both forms of communication technology require a third-party intermediary to facilitate the communication, and that third party can, to some extent, access the content of the communications.[100] Additionally, e-mail is as ubiquitous as the telephone, if not more so, in our daily communications. In *Katz*, the Court extended Fourth Amendment protection to telephone conversations, requiring law enforcement agents to procure a warrant before invading the caller's reasonable expectation of privacy by searching or seizing the contents of these communications through a wiretapping device.[101] More recently, the Ninth Circuit found a reasonable expectation of privacy in the contents of text messages despite their necessary transmission by a third-party service provider.[102] Private Internet activity, as the technological successor of the telephone, should receive the same protections.

Despite this, the third-party doctrine is often raised as a counter to the argument that there is a reasonable expectation of privacy in electronic communications. The third-party doctrine, as articulated in *United States v. Miller*, is the Fourth Amendment rule that information revealed to a third party will not be protected even if it was revealed on the assumption that "it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[103] Once information is revealed to a third party,

98. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (thermal-imaging scanner); *Riley*, 488 U.S. at 453 (low-flying helicopter).

99. *See* Kyllo, 533 U.S. at 34 (use of sense-enhancing technology not in general public use constitutes a search).

100. The mail also presents an analogous model, although postal workers do not have the same level of access to the contents of letters and packages. *See* United States v. Hernandez, 313 F.3d 1206, 1209–10 (9th Cir. 2002) ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior." (citations omitted)).

101. Katz v. United States, 389 U.S. 347, 359 (1967).

102. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (not reaching the question of whether there is a reasonable expectation of privacy in text messages).

103. United States v. Miller, 425 U.S. 435, 443 (1976).

the person revealing it loses his or her reasonable expectation of privacy in the contents of the communication.[104]

The analogy to telephone communications provides a useful conceptual tool and demonstrates why the third-party doctrine is an ill-founded challenge to the reasonableness of the expectation of privacy in electronic communications. While the Court in *Katz* did not explicitly analyze the ways in which a person's decision to use a form of technology accessible by the service provider might affect Fourth Amendment protections, it later made an important distinction for Fourth Amendment protections when it returned to telephone technology in *Smith v. Maryland*.[105] In choosing not to overrule *Katz* while leaving the numbers a person dials on their telephone unprotected, the Court recognized that, despite exposing the existence of their conversations to the phone company, people still retain a Fourth Amendment interest in the content of those communications.[106] While the Court in *Katz* held that "electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure,' . . . ."[107] the Court continues to avoid explicitly answering the question of whether a telephone user always has a reasonable expectation of privacy in the contents of his calls or text messages.[108] However, the content/non-content distinction as a barometer of reasonable expectation of privacy tracks the Court's jurisprudence and the idea can be usefully applied to the Internet context.

In *United States v. Warshak*,[109] the Sixth Circuit analogized Internet activity to telephone conversations, finding that the contents of electronic communications, whether carried over telephone lines or across the Internet, deserve Fourth Amendment protections, despite being revealed to the service provider. The district court found that "[t]he distinction between *Katz* and *Miller* makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on . . . nar-

104. *Id.*

105. 442 U.S. 735 (1979).

106. *Id.* at 741 ("[A] a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

107. Katz v. United States, 389 U.S. 347, 353 (1967).

108. City of Ontario v. Quon, 130 S.Ct. 2619, 2624 (2010) ("Though the case touches issues of far-reaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable.").

109. 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008) (vacating on grounds of ripeness).

rower questions than the general fact that the communication was shared with another."[110] While the decision was reversed en banc on procedural grounds, the Sixth Circuit's analysis provides a model for protecting the contents of private electronic communications despite concerns raised by the third-party doctrine. According to the Sixth Circuit, the Supreme Court's jurisprudence:

> recognize[s] a heightened protection for the CONTENT of the communications. Like telephone conversations, simply because the phone company or the ISP COULD access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.[111]

The Ninth Circuit also recognized the utility of the analogy to telephone technology, finding that government surveillance techniques that revealed the "to" and "from" addresses of an e-mail were "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*."[112] Only two other cases have addressed the Fourth Amendment's application to e-mail communications, and both found in favor of an e-mail user's reasonable expectation of privacy in his electronic communications.[113]

In an e-mail, just as in a telephone conversation, there are three parties: the two people involved in the conversation and the service provider. When a person sends an electronic communication to another person over the Internet, if that other person shares the contents of the communication with law enforcement agents, the communication is not protected by the Fourth Amendment. However, when an ISP or law enforcement agent monitors or intercepts that communication, an analogy should be drawn to the private communications protected in *Katz*.[114] In this scenario, the

110. *Id.* at 470.

111. *Id.* at 471.

112. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that monitoring IP address and to/from information of e-mails did not implicate Fourth Amendment).

113. *See* United States v. Long, 64 M.J. 57, 66–67 (C.A.A.F. 2006) (holding that a member of the Marine Corps may have a reasonable expectation of privacy in e-mails sent and received on a government computer); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that an e-mail user "enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant," but suggesting that "Internet e-mail" might receive different protections that the AOL e-mail communications in question).

114. The appellate court cases addressing Internet monitoring relied heavily on analogy to *Katz* and *Smith*. *See supra*, notes 109–12, and accompanying text.

other party to the conversation does not reveal anything or collude with law enforcement prior to receiving the communication. The contents of an e-mail, just like a conversation over the telephone, should be protected from the warrantless intruding eyes and ears of the service provider and law enforcement. Conversely, the non-content electronic information like the telephone pen registers that remain unprotected after *Smith v. Maryland*, should be accessible without warrant or probable cause.[115]

B. Warrantless Searches Bounded by Reasonableness

In the same year that *Katz* was decided, the Supreme Court also handed down *Camara v. Municipal Court*,[116] which redefined the relationship between reasonableness and probable cause. Whereas *Katz* and its progeny designate the warrant as the hallmark of a search's reasonableness, in *Camara* the Court gave reasonableness a foot in the door as an independent Fourth Amendment consideration.[117] The following year, the Court made this second Fourth Amendment strand explicit in *Terry v. Ohio*,[118] authorizing brief warrantless detentions supported only by an officer's reasonable articulable suspicion, and cursory outer garment searches (frisks) if the officer has reason to believe the suspect is armed and dangerous.[119] The reasonableness of a warrantless search depends on a court's balancing of "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree

Academics also argue in favor of this analogy. *See, e.g.*, Kerr, *supra* note 8, at 1038 ("The claim that rights in the contents of communications should be waived under the third-party doctrine does not work because the same argument could be made about telephone calls . . . . *Katz* established that the third-party doctrine does not apply in that setting.").

115. There is a debate over the usefulness of the content/envelope distinction for electronic communications. For an interesting survey of the issue, see Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009). Ultimately, however, it is outside the scope of this Note to decide whether the content/non-content distinction is a valuable framework for assessing the scope of Fourth Amendment protections because even those rejecting the analogy argue in favor of more, rather than less, protection than is currently provided for internet activity. *See, e.g.*, Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1453–55; Solove, *supra* note 7, at 1286–88.

116. 387 U.S. 523, 538 (1967).

117. *Id.*

118. 392 U.S. 1, 21 (1968).

119. Police may also conduct searches incident to lawful arrest without warrant. *See* Chimel v. California, 395 U.S. 752 (1969). This type of warrantless search is not relevant to the discussion of this Note because, at the time of an ISP's monitoring, no arrest has occurred.

to which it is needed for the promotion of legitimate governmental interests."[120]

In order for warrantless monitoring of private Internet activity to satisfy this Fourth Amendment test, the intrusion on a particular individual's privacy would have to be justified by a reasonable articulable suspicion at the moment the monitoring begins, and be reasonably related in scope to the circumstances which first justified the search.[121] In *Terry*, the initial stop was justified by the particularized suspicion that the appellant, Terry, was casing a store in contemplation of a robbery, and the governmental interest at stake was the potential danger to the law enforcement officer in his interaction with Terry.[122] No such particularized suspicion can be articulated when ISPs broadly monitor all of their subscribers' Internet activity using the tools provided by law enforcement to detect child pornography. Rather, this monitoring is more analogous to the broad programmatic searches discussed in the following section.[123]

Assuming *arguendo* that an ISP articulates a particularized and reasonable suspicion, the types of searches an ISP utilizes will not be reasonably related in scope as required by *Terry*.[124] An ISP can monitor the activity on its server in two ways: through shallow automated monitoring, or through "deep packet inspection."[125] Shallow automated monitoring restricts an ISP's view to network details, allowing it to see that communications are sent and received without access to its contents.[126] By its very nature this automated monitoring cannot be the result of a particularized suspicion. Furthermore, this level of shallow monitoring is unlikely to be of any use in the government's fight against child pornography.[127] Conversely, when a reasonable articulable suspicion is raised and an ISP initiates deep packet inspection directed towards a particular Internet account, the quantity of information accessible will be far beyond the scope of the suspicion that justified initiating the search. Deep packet inspection "refers to devices and technologies that inspect and take action based on the contents of the packet (commonly called the

120. United States v. Knights, 534 U.S. 112, 118–19 (2001) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

121. *Terry*, 392 U.S at 18.

122. *Id.* at 30.

123. *See infra* notes 130–46 and accompanying text.

124. 392 U.S. at 19 (requiring searches to be reasonably related in scope to the circumstances which justify them).

125. Ohm, *supra* note 116, at 1424–25, 1468.

126. *Id.* at 1468.

127. *See id.* ("Providers routinely argue that 'shallow packet' monitoring is insufficient to accomplish [their] goals.").

'payload') rather than just the packet header."[128] Through deep packet inspection, the entirety of each user's Internet communications is opened and accessible, not simply the "to" and "from" information. Additionally, deep packet inspections will likely be delimited by account information and Internet Protocol address (IP address), rather than by individual Internet user. Multiple people may use a computer that accesses the Internet through a particular service provider with a single IP address, creating further problems with the scope of the search.[129]

C. Warrantless and Suspicionless Searches

The Court is currently grappling with what standards to apply to this last category of searches. Although it appears that a "special need" apart from ordinary criminal law enforcement is required,[130] the methods for determining whether a special need exists are in flux. The searches carried out by ISPs, encouraged and facilitated by local and federal law enforcement, are without warrant and without suspicion. While the Court has created a category in which broad, suspicionless, programmatic searches may take place, sweeping searches of private Internet activity to detect child pornography do not meet the requirements established by the Court, whether carried out by law enforcement agents or ISPs.

In developing this third category, the Court again drew on the "reasonableness" language of the Fourth Amendment to determine when law enforcement agents may search without a warrant or even suspicion of wrongdoing.[131] However, the hallmark of a lawful warrantless and suspicionless search is that it must be motivated by a

128. DPACKET.ORG, *Introduction to Deep Packet Inspection/Processing*, https://www.dpacket.org/introduction-deep-packet-inspection-processing (last visited Feb. 16, 2011) (analogizing deep packet inspection to a postal worker opening an envelope and reading the letter inside).

129. *See, e.g.*, Kerr, *supra* note 8, at 1045–48 (arguing that the particularity requirement should apply to specific Internet users, rather than Internet accounts).

130. *See* New Jersey v. T.L.O., 469 U.S. 325, 351(1985) (Blackmun, J., concurring) (stating that a reasonableness balancing test should be applied "[only] in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable").

131. *See, e.g.*, Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing. While such suspicion is not an 'irreducible' component of reasonableness, we have recognized only limited circumstances in which the usual rule does not apply.").

primary purpose beyond the normal need for law enforcement.[132] Through this "special needs" doctrine the Court has supported routine border searches[133] and highway checkpoints designed to catch drunk drivers[134] and investigate traffic accidents.[135] When determining if a special need outside of ordinary law enforcement exists, courts will carefully scrutinize the rationale articulated for a particular program. In *Indianapolis v. Edmond,* the Court made it clear that a program designed to "detect evidence of ordinary criminal wrongdoing" does not constitute a special need and therefore falls outside this narrow exception to the Fourth Amendment's requirement of individualized suspicion.[136] A year later in *Ferguson v. City of Charleston*,[137] the Court struck down an alliance between law enforcement and hospital staff to root out cocaine use among pregnant patients. Despite the hospital's statement to the contrary, the Court determined that finding and arresting drug users had supplanted protecting the health of unborn children as the hospital's primary concern.[138]

If a court determines that the primary purpose of a search and seizure is not general law enforcement, it will engage in a balancing test to determine its reasonableness.[139] The reasonableness of a search depends on the "balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers."[140] The reasonableness of the accompanying seizure requires the court to consider "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[141] Only a search or seizure narrowly tailored to a pressing non-law enforcement need will pass the Court's test.

132. *Compare* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990) (ensuring roadway safety was the primary purpose of the checkpoint and therefore it did not violate the Fourth Amendment); *with Edmond*, 531 U.S. at 37 (a vehicle checkpoint established to find illegal narcotics is primarily a general law enforcement search and therefore violates the Fourth Amendment).

133. United States v. Martinez-Fuerte, 428 U.S. 543, 557 (1976) (finding that a special need exists in the protection of the integrity of United States borders).

134. *Edmond*, 531 U.S. at 39 (special need is the maintenance of roadway safety for other drivers).

135. Illinois v. Lidster, 540 U.S. 419 (2004).

136. *Edmond*, 531 U.S. at 38, 41–42.

137. 532 U.S. 67 (2001).

138. *Id.* at 81–84.

139. *See* Brown v. Texas, 443 U.S. 47, 50–51 (1979).

140. *Id.* at 50 (quoting Pennsylvania v. Mimms, 434 U.S. 106, 109 (1977)) (internal quotations omitted).

141. *Id.* at 51.

In determining the primary purpose of a warrantless programmatic search, the Court has either relied on the purpose as stated by law enforcement or gleaned the primary purpose from the record, as in *Ferguson*.[142] Justice Kennedy's concurrence in *Ferguson* focused on "substantial law enforcement involvement" during the planning and implementation of the program.[143] If asked, law enforcement and ISPs would be hard pressed to put forth a purpose for monitoring for child pornography that did not fall within the ambit of ordinary law enforcement. Unlike highway checkpoints, where the presence of a single drunk driver can compromise the safety of all drivers, the safety of Internet users as a whole is not at issue when monitoring for child pornography.[144] The Court has rejected the argument that the mere presence of child pornography on the Internet compromises its integrity and presents a broad risk to children.[145] When a broad programmatic search appears concerned with detecting unique instances of crime, as in the vehicle checkpoint for narcotics possession at issue in *Edmond*, a broader justification must be presented in order to satisfy the "special needs" requirement.[146] When ISPs or law enforcement agents monitor private Internet activity for evidence of child pornography trafficking, they do so with the primary purpose of rooting out individual child pornographers and pedophiles for arrest, not to protect the safety of the Internet for all users.

Even if a court somehow determined that monitoring the internet for evidence of child pornography fit within the standard of "special needs," the program would likely still fail the balancing test. While finding and prosecuting child pornographers certainly constitutes an issue of high public interest, the accompanying costs to the personal security of every Internet user are also grave. It is important to note that it is not the child pornographer's illegal conduct that this analysis seeks to protect, but rather everyone's right to engage in lawful activity without fear of government interfer-

142. 532 U.S. at 81–82.

143. *Id.* at 88 (Kennedy, J., concurring).

144. *See* Indianapolis v. Edmond, 531 U.S. 32, 39 (2000) (discussing the Court's rationale in *Sitz*: "This checkpoint program was clearly aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways, and there was an obvious connection between the imperative of highway safety and the law enforcement practice at issue.").

145. Ashcroft v. Free Speech Coal., 535 U.S. 234, 250 (2002) ("While the Government asserts that the images can lead to actual instances of child abuse . . . the causal link is contingent and indirect. The harm does not necessarily follow from the speech . . . .").

146. *Edmond*, 531 U.S. at 38.

ence. As Justice Brandeis wrote in his famous dissent in *Olmstead v. United States*, "the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him."[147] The decision to monitor private Internet activity for evidence of child pornography-related crimes implicates the privacy interests of all internet users. Given the pervasiveness of the Internet in all aspects of communication, business, and leisure, the public confidence in this vital technology would be greatly affected by the knowledge that at any point private conversations and Internet activity could be accessible to ISPs and law enforcement. Expectations of privacy and relative anonymity in Internet activity "are breached once ISPs begin monitoring, giving us the impression that we are always watched."[148] Eventually, "[p]ervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream," causing us to lose "the expression of eccentric individuality."[149]

IV.
ADDRESSING ARGUMENTS AGAINST THE WARRANT REQUIREMENT FOR INTERNET SEARCHES

As argued above, the analogy between the monitoring of private Internet activity and the *Terry* stop-and-frisk jurisprudence does not provide useful guidance in regulating ISP monitoring.[150] Similarly, ISP monitoring is unlikely to fit within the limitations imposed by the Supreme Court on special needs searches.[151] Therefore, this Note contends that only a warrant supported by probable cause can adequately protect Internet users' Fourth Amendment rights. While a warrant may be cumbersome, it is precisely this type of intermediate step that the serves to protect a person's private activity from unreasonable intrusion.[152] Congress recognized that a warrant or other protection should insulate private Internet activity from overzealous law enforcement when it enacted the Stored Communications Act.[153] However, as this Note will argue in the following section, law enforcement has circumvented these protections through the enlistment of ISPs, which have access to the

147. 277 U.S. 438, 476 (1928) (Brandeis, J., dissenting).

148. Ohm, *supra* note 115, at 1447.

149. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

150. *See supra* Part III.B, "Warrantless Searches Bounded by Reasonableness."

151. *See supra* Part III.C, "Warrantless and Suspicionless Searches."

152. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

153. 18 U.S.C. § 2703.

wealth of business and personal activity that takes place on the Internet, yet are not subject to the warrant requirements of the Fourth Amendment or the SCA. ISPs receive access to highly guarded hash values that they then use to examine every byte of electronic information that passes through their servers, violating people's reasonable expectation of privacy.[154] This section addresses several prevailing counterarguments in favor of keeping ISP monitoring outside the scope of the Fourth Amendment's warrant requirement.

A. Running Hash Values Is Not Sui Generis

As discussed above, there is a fourth category of law enforcement activity that the Supreme Court places outside the scope of the Fourth Amendment by declaring the action not to be a "search."[155] Some arguing against a warrant requirement for internet monitoring contend that the use of hash values, or "hashing,"[156] should not constitute a search at all, analogizing this technology to a dog sniff, something the Court has held is sui generis in its ability to detect only contraband.[157] However, in *United States v. Crist*,[158] the only case to directly address the Fourth Amendment's application to hashing, the court found that deriving the hash values of the defendant's computer and then comparing those values to known and suspected child pornography hash values both constituted searches violating the Fourth Amendment.

In *United States v. Place*[159] and *Illinois v. Caballes*,[160] the Supreme Court held that narcotics-sniffing dogs could be used without implicating the Fourth Amendment, because the dogs can only detect the presence or absence of contraband. The analogous argument for hashing runs as follows: there is no legitimate expectation of privacy in the possession of contraband; government conduct that reveals only the presence of contraband compromises no legitimate interests; a hash value search will only reveal the presence or absence of child pornography files.[161] However, several important

154. For a definition of hash values, see Salgado, *supra* note 67.

155. *See supra* note 73 and accompanying text.

156. *See* Salgado, *supra* note 66, at 44–46.

157. *See* United States v. Place, 462 U.S. 696, 707 (1983); Illinois v. Caballes, 543 U.S. 405, 409 (2005).

158. 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008).

159. 462 U.S. at 697–98.

160. 543 U.S. at 409.

161. Salgado, *supra* note 66, at 44–46; *see also* Orin Kerr, *District Court Holds that Running Hash Values on Computer Is a Search*, THE VOLOKH CONSPIRACY (Oct. 27, 2008, 100:11 AM), http://volokh.com/posts/1225159904.shtml ("If the hash is for

differences between the use of hash values and narcotics-sniffing dogs make this analogy unworkable. When the Supreme Court analyzed the use of narcotics-sniffing dogs, a key factor on which it relied was the idea of a dog as sui generis in its ability to detect only contraband.[162] While, like a drug-sniffing dog, child pornography hash values are designed to detect only contraband, the manner in which searches of Internet activity are carried out is fundamentally different. In running a hash, private electronic files must be opened, accessed, and copied, unlike a dog sniff that can permeate a closed suitcase or car trunk. A hash value program uses an algorithm to create unique identifiers for electronic files.[163] That program first makes a copy of every file on a suspect's computer or, in the case of ISP monitoring, every e-mail attachment and Internet file downloaded, and then creates a hash value for each file in order to compare them with child pornography hash values.[164] While hashing is designed to reveal only contraband files, the investigator running the hash program, unlike a trained canine, must copy and access each file in order to derive its unique hash value, even those in which a reasonable expectation of privacy remains, a process that could potentially reveal information about non-contraband files.[165] The fact that the ISP can choose to impose a limit on the scope of its search results is not sufficient for Fourth Amendment purposes.[166]

Additionally, the "dog sniff" line of cases takes place in the context of automobiles, which are subject to less Fourth Amendment protection.[167] By contrast, computers and Internet activity contain a

a known image of child pornography, then running a hash is a direct analog to a drug-sniffing dog.").

162. *Place*, 462 U.S. at 707; *Caballes*, 543 U.S. at 409.

163. Salgado, *supra* note 67, at 39.

164. Ty E. Howard, *Don't Cache out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet File*s, 19 BERKELEY TECH. L.J. 1227, 1232–34 (2004).

165. Marcia Hofmann, *Arguing for the Suppression of "Hash" Evidence*, CHAMPION MAGAZINE, May, 2009, *available at* http://www.nacdl.org ("[A canine search] does not expose non-contraband items that otherwise would remain hidden from public view . . . . A hash analysis, on the other hand, by its very nature requires the government to access files in order to derive their hash values, whether they are contraband or not, thus exposing data to which a client has a legitimate privacy interest.").

166. Katz v. United States, 389 U.S. 347, 356–57 (1967) ("[T]his Court has never sustained a search upon the sole ground that officers . . . voluntarily confined their activities to the least intrusive means . . . .").

167. Motor vehicles, partially because of their mobility, have become an exception to the warrant requirement of traditional Fourth Amendment jurispru-

record of the most intimate details of peoples' daily lives. People use computers as personal calendars, as well as to run businesses, store family photographs, and communicate with friends and family; in short, people use computers to do all of the things that the courts have determined make the home a special place, deserving the utmost Fourth Amendment protection.[168]

Another fundamental problem with applying the *Caballes* line of cases to hashing values arises from the use of hash values to rooting out child pornography specifically. The discussion in this section is partially premised on the idea that the hash values an ISP uses or receives from NCMEC are in fact hash values for contraband material. However, child pornography is not something that can be categorically determined; there is no chemical formula for child pornography, unlike drug contraband. While Congress has provided a definition of child pornography, it is nothing more than a series of attributes and therefore subject to significant judicial discretion.[169] Looking through an individual's private Internet activity for images that a single judge or jury has decided constitute child pornography is not necessarily a search for something intrinsically illegal to possess. As Richard Salgado explains, "[i]t is one thing to conclude that child pornography is contraband; it is quite another to conclude that a particular image to be included in a hash set is child pornography."[170] An image one court has determined meets the state or federal definition may not constitute child pornography in another jurisdiction, yet the file's hash value will be held in the NCMEC database and compared to private Internet files by ISPs. Determining which files contain known child pornography "requires exercise of discretion that is not required when teaching a dog to detect cocaine or developing a chemical test to react to particular narcotics."[171]

---

dence. *See, e.g.*, Carroll v. United States, 267 U.S. 132, 153 (1925) ("[I]t is not practicable to secure a warrant, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.").

168. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 38 (2001) (expressing concern that the thermal imaging technology in question might reveal "at what hour each night the lady of the house takes her daily sauna and bath . . . ."). Interestingly, in the Kyllo opinion, Justice Scalia observes that it does not matter whether or not a particular investigative technology ultimately reveals intimate details of private home life, simply that the technology has the potential to do so. *Id.* at 38–39.

169. *See* 18 U.S.C. § 2256(8) (defining child pornography). For a discussion of the fraught history of legislative and judicial efforts to define the boundaries of child pornography, see *supra* notes 20–36 and accompanying text.

170. Salgado, *supra* note 66, at 45–46.

171. *Id.* at 46.

In *Crist*, the district court found that deriving the hash values of the defendant's computer and then comparing those values to known and suspected child pornography hash values both constituted searches that violated the Fourth Amendment. However, the court's analysis is noticeably sparse and leaves out much of the underlying logic. While the government argued that running the hashing program on Crist's computer did not constitute a search because officers "didn't look at any files, they simply accessed the computer," the district court squarely disagreed.[172] "By subjecting the entire computer to a hash value analysis—every file, internet history, picture, and 'buddy list' became available for Government review. Such examination constitutes a search."[173] The court also held that comparing the hash values derived in the preceding forensic analysis to known or suspected child pornography hash values constituted an additional search entitled to Fourth Amendment limitations.[174]

Other courts have also suggested that hashing may constitute a search in certain contexts.[175] While the Ninth Circuit in *United States v. Borowy* determined that the defendant negated his reasonable expectation of privacy by using a file-sharing program, the court noted that where a person maintained a reasonable expectation of privacy and "the government 'vacuumed' vast quantities of data indiscriminately—we might find a Fourth Amendment violation."[176] In another case, the court similarly noted that hash algorithms and "similar search tools may not be used without specific authorization in the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized."[177]

Even academics arguing against including hash values within Fourth Amendment protections recognize the ramifications of their position.[178] Academics have noted that, following the dog-sniff sui generis logic, the more tailored to detecting contraband a technology becomes, "the less the public can reasonably expect the law

172. United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008).

173. *Id.*

174. *Id.* at 586–87.

175. United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010); United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009).

176. *Borowy*, 595 F.3d at 1048–49 n.2.

177. *Comprehensive Drug Testing*, 579 F.3d at 999.

178. Salgado, *supra* note 66, at 45 ("Certainly we benefit from an aggressive battle against the scourge of child pornography. Yet there would be something very creepy about an expansive and unrestrained search through media, even though properly in the hands of law enforcement, for offending images.").

to protect them against government intrusions."[179] Despite Richard Salgado's view that hashing should not constitute a search, he nevertheless expresses concern that his position might lead to searches for contraband based on warrants for completely unrelated criminal activity.[180] Searches of anyone or anything based on "police hunches, whims, prejudices, or anything at all . . . are beyond the purview of the Fourth Amendment" so long as the technology facilitating the search detects only contraband.[181] Doubtless, this is a level of "Big Brother" interference by which few are willing to abide.[182] Reliance on the "nothing to hide" argument would allow ISPs to initiate hashing programs that cull through each and every file on their server in order to detect contraband material, while in the process exposing those files in which Internet users continue to maintain a reasonable expectation of privacy. Furthermore, this "nothing to hide" retort masks the destruction of what Daniel Solove argues is the social value of privacy, the "protection of the individual based on society's own norms and values."[183] This societal harm is added to the harm experienced by the individual whose Fourth Amendment rights are violated. Privacy exists, not in opposition to society's interests, but rather as an integral expression of them.[184]

B. Internet Users Do Not Meaningfully Consent to Monitoring

Another potential argument against requiring a warrant before the government may request ISP monitoring of their subscribers' Internet activity focuses on the privacy policy that every user must agree to before accessing their internet services. Consent is a fundamental principle in contract law, and there is a presumption of meaningful consent to a contract's terms.[185] While many scholars feel that the existence of a consent form should not be determinative,[186] courts generally accept the enforceability of standard form

179. Hofmann, *supra* note 165.

180. Salgado, *supra* note 66, at 45.

181. Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. DAVIS L. REV. 781, 823–24 (2008).

182. Big Brother is a fictional dictator who mandates complete surveillance of all citizens. GEORGE ORWELL, 1984 (1949).

183. Daniel J. Solove, *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 763 (2007).

184. *Id.*

185. *See* Brian Bix, *Contracts*, *in* THE ETHICS OF CONSENT 251 (Franklin G. Miller & Alan Wertheimer eds., 2010).

186. *See, e.g.*, E. Allan Farnsworth, CONTRACTS § 4.26, at 296–97 (3d ed. 1999) (discussing how the dangers inherent in standardization are further increased

contracts, or contracts of adhesion, only holding them unenforceable where a particular term is "unconscionable."[187] However, courts enforcing these "take-it-or-leave it" contract terms often rely on the consumer's ability to return the product after disapproving of the contract's terms.[188] Where the consenting party has no reasonable alternatives or choices relating to a particular term among different contractual providers, courts' reliance on a consumer's ability to find a better offer seems misplaced.[189]

Paul Ohm presents what he terms the "proximity principle" as a way to assess the legitimacy of an Internet service subscriber's consent.[190] Ohm looks to the "level of competition for the service provided" and the "nature of the channels of communication between the provider and customer."[191] By assessing whether users have a meaningful choice among ISPs and looking at the mechanisms ISPs use to ask for and receive consent, the nature of the so-called consent becomes clearer.[192] Compared to the variety of e-mail providers, there is relatively little choice between Internet providers. Therefore, a customer is limited in his or her ability to shop around to find the privacy policy that best suits his or her needs. The market has not, and likely will not, solve for this lack of privacy alternatives, because "ISPs have a great motive to pay a little more attention than they have before to their users' secrets. By doing so, they can tap new sources of revenue, which given their precarious situation, may be the only way they can guarantee their survival."[193] Ohm also highlights a problem with the knowledge aspect of in-

when parties are in unequal bargaining positions and terms are take-it-or-leave it); Bix, *supra* note 185, at 253–54 (noting that validity of consent depends on factors such as actual knowledge of terms and reasonable alternatives).

187. Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569 (1st Dep't 1998); U.C.C. § 2-302 (2005).

188. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452–53 (7th Cir. 1996).

189. *See* Bix, *supra* note 185, at 253–54. For an example of a court recognizing that consumers may lack meaningful alternatives, see *Henningsen v. Bloomfield Motors*, 161 A.2d 69 (N.J. 1960).

190. Ohm, *supra* note 115, at 1475–77.

191. *Id.* at 1475.

192. Bix, *supra* note 185, at 252 ("[T]here is a relative lack of consent in the sense that there may be no reasonable alternatives to entering the transaction in question.").

193. Ohm, *supra* note 115, at 1425. *See id.* at 1426 (ISPs monitor Internet activity to track and block overuse that congests the network and provide directed advertising); *see also* Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICH. L. REV. 837, 843 (2006) ("In insufficiently competitive industries, businesses can afford to lose the small cadre of readers and dictate onerous terms to the nonreaders.").

ternet users' consent: the privacy policy rarely receives customer approval before the customer subscribes to the services.[194] Rather, after subscribing—usually over the phone—the user often receives a copy of the privacy policy with the first bill.[195] These factors seem to suggest that the consent ISPs receive to monitor their users' private Internet activity is not meaningful.

Assuming *arguendo* that customers consent to ISP monitoring based on their acceptance of contracts of adhesion, an examination of several major ISPs' contracts reveals little detail about the frequency and depth of monitoring to which a customer must agree. While contracts of adhesion can be supported by meaningful consent, it is less clear that a customer can consent to something not fully detailed in their customer agreement or privacy policy. For example, the Verizon Wireless customer agreement states: "[w]e collect personal information about you. We gather some information through our relationship with you, such as information about the quantity, technical configuration, type, destination and amount of your use of our telecommunications services."[196] While indicating that personal information is collected, the casualness belies the depth and breadth of monitoring that an ISP has the capacity to engage in. Other major ISP privacy notices and customer agreements contain similar generalized descriptions.[197] The Comcast customer privacy notice explains that the company collects its customers' information "at several different points when you initiate and use our services."[198] The policy then goes on to list a series of categories of information that it may collect, but notes that it is not exhaustive, or even typical, of the range of information collected.[199] A customer's consent to ISP actions that are not explicitly included in a contract seems problematic.

194. Ohm, *supra* note 115, at 1477.

195. *Id.*

196. *Verizon Wireless Customer Agreement*, VERIZON WIRELESS, http://www.verizonwireless.com/customer-agreement.shtml (last visited Sept. 19, 2011).

197. *See, e.g.*, *AT&T Privacy Policy*, AT&T, http://www.att.com/Common/about_us/privacy_policy/print_policy_aug2009.html (last visited Feb. 16, 2011); *Time Warner Cable Subscriber Privacy Notice*, TIME WARNER CABLE (July 2010), http://help.twcable.com/html/twc_privacy_notice.html (failing to mention the ability to monitor Internet activity; mentioning only that monitoring may occur for email).

198. *Comcast Customer Privacy Notice*, COMCAST COMMC'NS CORP. (Jan. 1, 2009), https://www.comcast.com/MediaLibrary/1/1/Customers/Customer_Support/Legal/Q3PrivacyPolicyUniLegalStndENG.pdf.

199. *Id.*

V.
DEPUTIZING ISPS

Searches carried out by private citizens do not immediately implicate the Fourth Amendment.[200] However, the Supreme Court has developed a jurisprudence "guided by common law agency principles"[201] in which an individual acts as an agent of the state if "the government knew of and acquiesced in the intrusive conduct, and . . . the party performing the search intended to assist law enforcement efforts . . . ."[202] This section will argue that the SCA and related anti-child pornography statutes effectively deputize ISPs without extending statutory or constitutional protections to their activities.

While the SCA does not require ISPs to monitor and report criminal activity that takes place on their servers, the inquiry does not end there.[203] Law enforcement agents at both the federal and state level have encouraged and facilitated ISP monitoring in such a way that ISPs act as the functional equivalent of a government agent when monitoring subscribers' Internet activity. In authorizing the NCMEC to make highly guarded child pornography hash values available to ISPs, the federal government facilitates the intrusive monitoring of private Internet activity.[204] State law enforcement agents similarly encourage ISPs to monitor broadly in ways that they themselves legally could not.[205] By using these hash values and other monitoring software, ISPs actively assist law enforcement efforts without being subjected to constitutional or statutory limitations.

A. Government Knows of and Acquiesces in Intrusive Conduct

While there is no bright line test that "distinguishes instances of 'government' conduct from instances of 'private' conduct," when deciding whether a government official knows of and acquiesces in a private party's search, courts will look for such indicators as "in-

200. United States v. Jacobson, 466 U.S. 109 (1984).

201. United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010).

202. United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).

203. *See, e.g.*, Skinner v. Railway Labor Execs.'s Ass'n, 489 U.S. 602, 615 (1989) ("The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one. Here, specific features of the regulations combine to convince us that the Government did more than adopt a passive position toward the underlying private conduct.").

204. *See* PROTECT Our Children Act of 2008, Publ. L. No. 110-401, 112 Stat. 4229 (to be codified at 18 U.S.C. § 2258C(a)(1)–(2)).

205. *See infra* notes 211–17 and accompanying text.

stances of police-private citizen contact" and whether the police instigated the search.[206] In *Skinner v. Railway Labor Executives's Association*, the government demonstrated its "encouragement, endorsement, and participation" by "remov[ing] all legal barriers" and exhibiting a "strong preference for testing" and "its desire to share the fruits of such intrusions."[207] The Court explained that a lack of overt compulsion by the government would not be determinative; rather, "specific features of the regulations combine to convince us that the Government did more than adopt a passive position toward the underlying private conduct."[208] As this section will show, the government has both exhibited a strong preference for Internet monitoring and statutorily mandated that ISPs share the fruits of their searches; and rather than remove legal barriers, the government exploits an area in which few legal barriers exist.

The DOJ's Community Oriented Policing Guide (COPS Guide) on combating Internet child pornography notes, "there is often a lack of specific legislation setting out ISPs' obligations. This makes it especially important for police to establish good working relations with ISPs to elicit their cooperation."[209] Law enforcement recognizes the competition among ISPs fighting to control access to a highly prized commodity, and can effectively manipulate this pressure to their own ends. Failure to comply with law enforcement by monitoring and restricting access to objectionable online material might tarnish the IPS's commercial reputation and lead to loss of business.[210]

Andrew Cuomo, the former Attorney General for the State of New York, is a prime example of how law enforcement may effectively exploit these conflicting interests in order to force ISPs to monitor their users' activity in a way that—without a warrant or other procedural protection—law enforcement cannot. In June 2008, Cuomo convinced three major service providers—Verizon, Sprint, and Time Warner Cable—to block their users from accessing websites that feature pornographic images involving children.[211] The three providers also agreed to contribute a collective

206. *Miller*, 688 F.2d at 656–57.

207. *Skinner*, 489 U.S. at 615–16.

208. *Id.* at 615.

209. COPS GUIDE, *supra* note 13, at 36.

210. *See, e.g.*, *Email ISPs*, N.Y. STATE ATT'Y GEN., http://nystopchildporn.com/email_isp.html (last visited Apr. 20, 2011) (including a list of non-compliant ISPs with form letters for subscribers to send to urge compliance with Andrew Cuomo's monitoring requirements).

211. *See* Press Release, N.Y. State Att'y Gen., Attorney General Announces Deal with Nation's Largest Internet Service Providers (June 10, 2008), http://

$1.125 million to the New York State Office of the Attorney General and NCMEC in their efforts to combat child pornography.[212] Cuomo was able to elicit cooperation from ISPs, who have generally preferred a *laissez-faire* approach to monitoring user content, by threatening the ISPs with charges of fraud and deceptive business practices and maintaining a published list of non-compliant ISPs to shame disobedient providers into compliance.[213] In order to avoid consumer backlash and potential liability in seemingly foundationless lawsuits,[214] ISPs had to sign a code of conduct developed by the Attorney General that outlines their monitoring and website-blocking duties.[215] All of these actions taken together should constitute law enforcement's knowledge of and acquiescence in the ISPs' intrusive searches, if not their outright compulsion. In 2004, a federal Pennsylvania district court struck down the Pennsylvania legislature's attempt to statutorily require ISPs to block access to these same websites.[216] While New York technically does not require ISPs to monitor and restrict their users' access, the result is functionally the same.[217]

Law enforcement encouragement and strong-arm tactics compel ISPs to monitor their subscribers' Internet activity. The release of once highly guarded hash values for child pornography files provides the tools necessary to do so. The PROTECT Our Children Act authorizes NCMEC to provide ISPs with hash values and other unique identifiers so that ISPs can catch those transmitting child pornography and report the activity to law enforcement.[218] The

www.nystopchildporn.com/press_releases/2008/june/10a.html; Danny Hakim, *3 Net Providers to Block Sites With Child Sex*, N.Y. TIMES, June 10, 2008, at A1, *available at* http://www.nytimes.com/2008/06/10/nyregion/10internet.html.

212. Press Release, N.Y. State Att'y Gen., *supra* note 211.

213. Hakim, *supra* note 211.

214. *See* Letter from Att'y Gen. Andrew Cuomo to Comcast Gen. Counsel (July 21, 2008), *available at* http://www.dslreports.com/r0/download/1330518~ac9e421e02d7f4fb5de858f3fa4515ac/CuomoComcast.pdf [hereinafter Cuomo Letter] (threatening "legal action" for failure to sign the code of conduct).

215. *See Shutting Down the Internet Child Pornography Pipeline*, N.Y. STATE ATT'Y GEN., http://www.nystopchildporn.com (last visited Apr. 20, 2011).

216. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (holding that 18 Pa. Const. Stat. §§ 7621–7630 (2002) violated the First Amendment).

217. Comcast was the only major ISP to balk at Attorney General Cuomo's request to begin monitoring its users' Internet activity. In response, Cuomo threatened the company with a lawsuit for unspecified violations. *See* Cuomo Letter, *supra* note 214. Several minor ISPs have not signed onto Attorney General Cuomo's code of conduct. *See* N.Y. STATE ATT'Y GEN., *supra* note 210.

218. PROTECT Our Children Act of 2008, Publ. L. No. 110-401, 112 Stat. 4229 (to be codified at 18 U.S.C. § 2258C(a)(1)–(2)).

statute does not mandate that ISPs use these hash values to monitor the traffic on their servers; however, as the Court made clear in *Skinner*, this is not required for deputization.[219] Hash values for child pornography files serve no purpose outside of monitoring Internet activity and blocking objectionable material, and the federal government's decision to provide these hash values to ISPs surely constitutes more than "adopt[ing] a passive position."[220] For example, while the COPS Guide does not detail the type of cooperation sought from ISPs, it recognizes that in the fight against Internet child pornography, ISPs occupy a vital position with complete access to the pipeline of information that travels across the Internet. With DOJ support, Microsoft recently released PhotoDNA, a program designed to block access to websites with child pornographic material, designed by utilizing NCMEC hash values.[221] While PhotoDNA's developers insist "they don't want to see it evolve into a filtering system that's mandated by the government," the government's track record in this area should be cause for concern.[222] Because Microsoft has made the program freely available to other service providers, there is little preventing the government from engaging in a Cuomo-like campaign of forced compliance. The federal government first provides ISPs with access to the child pornography hash values stored by NCMEC and Microsoft's PhotoDNA, and after providing ISPs with this "key," any local law enforcement effort to "elicit cooperation" must certainly rise to the level of knowledge and acquiescence in any subsequent ISP monitoring.

Additionally, by criminalizing the failure to report "actual knowledge of any facts or circumstances" related to child pornography,[223] one can see how an ISP might be prosecuted for failure to take advantage of programs that would provide them with actual knowledge.[224] As Congressman Nick Lampson said in support of a

219. *See* Skinner v. Railway Labor Execs.'s Ass'n, 489 U.S. 602, 615 (1989) (finding that railways authorized to perform breath and urine tests on employees were not engaging in private searches, even though they were not mandated to do so).

220. *Id.*

221. Martin Kaste, *A Click Away: Preventing Online Child Porn Viewing*, NPR (Aug. 31, 2010), http://www.npr.org/templates/story/story.php?storyId=129526579.

222. *Id.*

223. PROTECT Our Children Act of 2008, Publ. L. No. 110-401, 112 Stat. 4229 (to be codified at 18 U.S.C. § 2258C(a)(1)–(2)).

224. The Fourth Circuit recently held that fear of punishment alone was not enough to deputize an ISP. United States v. Richardson, 607 F.3d 357, 367 (4th

bill to statutorily ratchet up the penalties for an ISP's failure to report complaints of child pornography on its servers, "[i]f we can encourage—and certainly a fine would be an encouragement—the ISP to be in a position to give the information to law enforcement, we are encouraging them to be on the side of law enforcement . . . ."[225] Others have also noted how this pressure will operate to turn ISPs into virtual "child porn cops."[226]

B. ISPs Search with the Intent to Assist Law Enforcement

Deputization of a private actor involves the convergence of law enforcement intent and the intent of the private actor.[227] It is not enough to encourage a third party to undertake a search beneficial to law enforcement if that third party does not intend to assist law enforcement. A private search will be subject to Fourth Amendment restrictions where the conduct has "as its purpose the intention to elicit a benefit for the government in either its investigative or administrative capacities."[228] ISPs have many reasons outside of law enforcement to monitor the activity of their users, such as to earn money through targeted advertising or trace high-bandwidth users who slow their services;[229] however, the type of monitoring required to be of use to law enforcement in their fight against online child pornography can serve no other purpose.

Courts often face difficulties when dealing with the "intent to assist law enforcement" prong because people rarely operate with a single motivation at any given moment. While some circuits have allowed the intent to assist law enforcement to coexist with a "legitimate independent motivation" without violating the Fourth Amendment, this independent motivation must be closely examined;[230] preventing criminal activity is not a sufficiently indepen-

Cir. 2010) (defendant asserted that America Online's decision to monitor his Internet activity and report the presence of child pornography to NCMEC's Cyber Tip Line constituted government action). However, the court examined the idea of deputization in the pre-PROTECT Our Children Act landscape and AOL detected Richardson's child pornography through its own cache of hash values. *Id.* at 360, 362–63.

225. Hakim, *supra* note 211.

226. Bill Dedman & Bob Sullivan, *ISPs Pressed to Become Child Porn Cops*, MSNBC (Oct. 16, 2008), http://www.msnbc.msn.com/id/27198621.

227. *See* United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (government must acquiesce in conduct and private citizen must intend to aid law enforcement).

228. United States v. Attson, 900 F.2d 1427, 1431 (9th Cir. 1990).

229. Ohm, *supra* note 115, at 1422–27, 1462–68.

230. United States v. Reed, 15 F.3d 928, 931–32 (9th Cir. 1994) (rejecting the government's contention that a hotel employee searched the room to ensure that

dent motivation.[231] The Supreme Court has not yet addressed how an actor's motivation should be assessed, and the circuit courts have tackled the issue in different ways.[232] However, ISP monitoring of private internet activity for evidence of child pornography satisfies each test proposed by the circuit courts.

The Sixth and Ninth Circuits take the approach least favorable to the government by requiring that the private actor's intent be "entirely independent of the government's intent to collect evidence for use in a criminal prosecution" to avoid implicating the Fourth Amendment.[233] Where a private actor has a "legitimate independent motivation," the Fourth Amendment will not apply.[234] An ISP that monitors pursuant to Andrew Cuomo's ISP Code of Conduct does so knowing that the information it furnishes to the government will likely be used in a criminal prosecution. Even if the argument could be made that an ISP engaged in deep packet inspection for their own purposes, the knowledge that evidence of child pornography must be turned over to law enforcement prevents the ISP from acting completely independent of the government's desire to collect evidence under the Sixth Circuit test.

The Tenth Circuit collapses the two-prong assessment into a single inquiry by examining the government's role in the search as a means to uncover the private actor's primary purpose. If the government was involved "directly as a participant . . . or indirectly as an encourager," then the private actor likely intended his search to assist law enforcement.[235] While the government does not participate in ISP monitoring, the government certainly can be said to encourage the searches by providing hash values (the means necessary to effectively monitor Internet activity for child pornography). Courts will often examine other possible proxies for the private actor's intent, including "whether the private actor acted at the request of the government and whether the government offered the private actor a reward," as well as whether the private actor contacted the police prior to the search or collected evidence to turn

there was no damage to hotel property). The "legitimate independent motivation" articulation comes from *United States v. Walther*, 652 F.2d 788, 792 (9th Cir. 1981).

231. *Reed*, 15 F.3d at 931–32.

232. *See infra* notes 233–36.

233. United States v. Bowers, 594 F.3d 522, 526 (6th Cir. 2010) (quoting United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008)) (internal quotations omitted); *Attson*, 900 F.2d at 1432–33.

234. *Walther*, 652 F.2d at 792; *Attson*, 900 F.2d at 1432–33.

235. United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996).

over to law enforcement.[236] Though not offered a reward, ISPs offering their services in New York, for example, must comply with the Attorney General's monitoring program and turn over any evidence found or face public embarrassment.

Ultimately, these different tests reflect the Fourth Amendment value of protecting individuals from unnecessary intrusion by government actors, and therefore focus on "whether the governmental involvement is significant or extensive enough to objectively render an otherwise private individual a mere arm, tool, or instrumentality of the state."[237] Law enforcement needs the cooperation of ISPs in order to effectively tackle the problem of child pornography trafficking and accordingly both encourages and facilitates ISPs' monitoring. This monitoring provides ISPs with no benefit apart from the avoidance of the bad publicity that non-compliance might bring.

The Supreme Court's jurisprudence in determining the "primary purpose" in special needs cases also provides a useful framework to assess private actor motivations. In *Ferguson v. City of Charleston*,[238] the Court determined the purpose of the Medical University of South Carolina's alliance with local law enforcement by examining the program's development and procedural mechanisms.[239] Examining the level of cooperation between ISPs and law enforcement before and during the ISPs' monitoring reveals a coordinated alliance instigated by government intervention. Not until Cuomo engaged in bullying and created incentives did ISPs engage in wholesale monitoring for child pornography. In his concurrence in *Ferguson* Justice Kennedy wrote, "[t]he traditional warrant and probable-cause requirements are waived . . . on the explicit assumption that the evidence obtained in the search is not intended to be

236. United States v. Ginglen, 467 F.3d 1071, 1074 (7th Cir. 2006) (citing United States v. Shahid, 117 F.3d 322, 325 (7th Cir. 1997)); *see also Walther*, 652 F.2d at 792.

237. State v. Kahoonei, 925 P.2d 294, 300 (Haw. 1996) ("In so doing, we focus on the actions of the government, because . . . the subjective motivation of a private individual is irrelevant.").

238. 532 U.S. 67 (2001).

239. *Id.* at 81–82. While *Ferguson* did not the reach the question of when a private actor becomes a state agent because the hospital, as a public institution, was already considered a state actor, the Court placed enormous emphasis on what Justice Kennedy called "substantial law enforcement involvement" in the planning and implementation of the program. The participation of law enforcement at all stages of the hospital's drug testing program belied the hospital's contention that their primary purpose was the health and safety of their patients. *Id.* at 88 (Kennedy, J., concurring).

used for law enforcement purposes."[240] This is a tenuous position to maintain in the case of ISP monitoring, given that the federal government provides ISP with child pornography hash values and statutorily requires ISPs to turn over any evidence of child pornography.[241] The government freely gives ISPs the tools to Internet monitoring for child pornography, publicly shames ISPs that do not use these tools, and statutorily requires ISPs to turn over anything found as a result.

C. Other Third-Party Statutory Reporting Requirements

This argument is not intended to call into question any other statutory reporting requirements, such as those for doctors,[242] hospitals,[243] or teachers.[244] These other statutory reporting requirements differ from those imposed on ISPs in several important ways. A key factor relied on in the argument that ISPs have been deputized is that the PROTECT Our Children Act provides child pornography hash values to ISPs, thereby enabling the monitoring of its users' private Internet activity for evidence of child pornography.[245] No similar information sharing happens in other statutorily-required reporting schemes. The federal government does not provide doctors with a means to sort through potential patients to identify those who may commit a crime. Hospitals, doctors, and teachers report information gathered in the course of their ordinary business practices. Statutory reporting requirements alone will not deputize these professionals. Rather, the argument is that they, like ISPs, can neither actively seek out the information at congressional or law enforcement's behest nor use tools provided by the government to that end.

240. *Id.* at 88 (Kennedy, J., concurring).

241. *See* 18 U.S.C. § 2258A(a) (2006).

242. *See, e.g.*, Am. Med. Assoc., Council on Ethical and Judicial Affairs, Code of Medical Ethics, Op. E-5.05 (2007), *available at* http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.page? (requiring reporting "when a patient threatens to inflict serious physical harm to another person or to him or herself and there is a reasonable probability that the patients may carry out the threat").

243. *See, e.g.*, ARK. CODE ANN. § 12-12-602 (2010) (requiring reporting of intentionally inflicted knife or gunshot wounds).

244. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-3620 (2011) (requires "any . . . person who has responsibility for the care or treatment of [a] minor" to report suspected abuse or neglect to a peace officer or child protection agency).

245. PROTECT Our Children Act of 2008, Publ. L. No. 110-401, 112 Stat. 4229 (to be codified at 18 U.S.C. § 2258C(a)(1)–(2)).

Even if other private actors were somehow turned into government agents by their respective statutory reporting requirements, the third-party doctrine[246] and "special needs" justification for programmatic searches[247] present reasonable challenges to any argument that doctors, teachers, and others violate the Fourth Amendment. In these examples the third-party doctrine becomes a much more reasonable objection. A child who reveals to a teacher that her parents abuse her loses any reasonable expectation of privacy by sharing the information with another. This differs from the communication between two private actors intercepted by an ISP, because the information was never intentionally shared with the ISP.

The existence of a special need outside of law enforcement also appears much more plausible in these other statutory reporting contexts. A hospital reporting an intentional gunshot wound to local police is analogous to a highway traffic stop to gather evidence about a recent car accident. In *Lidster* the Court explained that the law ordinarily allows the police to seek information about a specific crime from members of the public, differentiating between searches with the goal of individualized crime control and those with more generalized crime control goals.[248] A doctor who reports that her patient confessed contemplating harm to another person would not likely be characterized as facilitating generalized crime control, but rather expressing concern about a unique instance of future criminal activity.[249]

CONCLUSION

Congress and law enforcement agents have unfortunately been too zealous in their efforts to address the scourge of child pornography and the ways in which the Internet has allowed its transmission to flourish. The continued existence of child pornography presents very real dangers to minors in the United States and around the world. However, efforts to eradicate this problem should not come at the expense of the privacy interests of all In-

246. United States v. Miller, 425 U.S. 435, 443 (1976). For a description of the third-party doctrine, see *supra* notes 103–04 and accompanying text.

247. Indianapolis v. Edmond, 531 U.S. 32, 36 (2000).

248. Illinois v. Lidster, 540 U.S. 419, 424-425 (2004).

249. This is analogous to the circumstances in which many courts refuse to allow private actions under the Fourth Amendment. *See, e.g.*, United States v. Ginglen, 467 F.3d 1071, 1075 (7th Cir. 2006) (brothers entered a home to protect their father); United States v. Shahid, 117 F.3d 322, 326 (7th Cir. 1997) (mall security guard acted to protect the safety of the mall).

ternet users. The Internet has become a fundamental medium for expression and communication. However, the extent to which private Internet activity must be monitored in order to effectively combat the presence of child pornography has the potential to seriously chill people's willingness to utilize the Internet freely.

Private Internet activity fits squarely within the type of activity that the courts and Congress have sought to protect from unreasonable searches and seizures by law enforcement.[250] The prominence of the Internet in our daily lives suggests that a user's subjective expectation of privacy is in fact reasonable.[251] The Supreme Court's jurisprudence in other technology-based Fourth Amendment questions indicates that an Internet user does not forgo this reasonable expectation of privacy by relying on a third-party provider to facilitate communications.[252] Furthermore, the lack of meaningful choices between ISPs and delayed access to the contents of privacy policies vitiates any consent to closely monitor one's usage that users might give ISPs.

The statutory framework of the SCA and PROTECT Our Children Act creates an environment ripe for law enforcement to coerce ISPs to monitor the activity on their servers for evidence of child pornography without the limitations of the Fourth Amendment or statutory protections. State and federal law enforcement offices have in fact seized these opportunities, and by their actions turned ISPs into governmental agents for purposes of monitoring and reporting child pornography. This argument is not presented in an effort to protect the conduct of pedophiles and child pornographers, but rather to draw attention to the serious undermining of the privacy under the Fourth Amendment every Internet user faces. Since the SCA requires badge-wearing law enforcement officers to procure a warrant or other magisterial document before accessing stored electronic communications,[253] ISPs should be subject to the same requirements when they search to aid law enforcement.

Unfortunately, this problem will likely not receive serious attention in litigation until Congress amends the SCA to incorporate a suppression remedy. The inclusion of a suppression remedy will provide defense attorneys with incentive to protect their clients'

250. *See, e.g.*, Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

251. *See supra* note 93 and accompanying text.

252. *See, e.g.*, *Katz*, 389 U.S. 347.

253. 18 U.S.C. § 2703.

Fourth Amendment rights as well as restoring the public's faith in government accountability in Internet "surveillance practices and replace general anxiety about Big Brother online with a more focused attention on actual instances of misconduct."[254] While suppression remedies necessitate the guilty going free in instances of government misconduct or mistake, without a suppression remedy, the contours of appropriate government conduct remain unclear. In the absence of a legislative amendment, attorneys should be encouraged to appeal the decision on constitutional grounds. Because child pornography presents a serious offense to the sensibilities of most Americans, Congress remains under enormous pressure to take a hard line in criminalizing the behavior and fostering prosecution of child pornographers, giving short shrift to potential constitutional problems. This makes a Supreme Court decision on the constitutionality of the SCA and PROTECT Our Children Act all the more pressing. Until this issue receives the judiciary's attention, the legislative and executive branches will continue to subject millions of Internet users to Fourth Amendment violations.

254. Kerr, *supra* note 6, at 840–41; *see also* Solove, *supra* note 7, at 1299.