CHILD PORNOGRAPHY, THE INTERNET, AND THE CHALLENGE OF UPDATING STATUTORY TERMS

I. INTRODUCTION

It is uncontroversial that the formal power to define federal crimes resides exclusively with Congress.[1] But federal criminal statutes are often sufficiently broad or indefinite that it is left to the courts to clarify what a particular law will mean in practice.[2] Courts make criminal law more definite in many ways, including by determining what facts are sufficient to establish the substantive and mens rea elements laid out in the statutory text. Federal courts have engaged in this type of crime definition in the field of child pornography law. In doing so, they have corrected imprecision in the statute's text and engaged in an ongoing process of law development that has proved responsive to the changing nature of the underlying behavior that the statute criminalizes.

Since its inception, the federal child pornography act has included the mens rea term "knowingly" in defining each of the offenses prohibited by 18 U.S.C. § 2252.[3] Congress intended the mens rea term to help prevent the prosecution and conviction of inadvertent recipients of illicit materials. In the years since the statute was drafted, the expansion of personal computer ownership and internet use have fundamentally transformed the ways in which child pornography is collected and exchanged, increasing the likelihood of mistaken receipt. The mens rea term "knowingly" is sufficiently flexible to accommodate this technological change and to continue to serve the purpose for which Congress intended it — distinguishing between innocent and culpable conduct. Many courts have quietly but adeptly made the necessary updates to the statute by refining the evidentiary standards they use to define the statutory elements in more concrete terms. Some aver that the statute has outlived its usefulness and that courts are impermissibly performing a legislative task through their sufficiency-of-the-evidence jurisprudence.[4] This Note argues that courts' evidentiary standards help to implement congressional intent by protecting accidental or mistaken recipients while retaining the capacity to prosecute and convict truly culpable offenders. Courts are not only competent to

---

[1] *See, e.g.*, Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469, 471 (1996) (citing Whalen v. United States, 445 U.S. 684, 689 (1980)).

[2] *Id.*

[3] 18 U.S.C. § 2252 (2006); Protection of Children Against Child Exploitation Act of 1977, Pub. L. No. 95-225, § 2252, 92 Stat. 7, 7–8 (1978).

[4] *See, e.g.*, United States v. Polizzi, 549 F. Supp. 2d 308, 357–58 (E.D.N.Y. 2008).

ensure that the statute continues to operate effectively in light of new factual circumstances, but they also have an obligation to make the necessary adjustments in the absence of explicit congressional revision of the statute.[5]

Part II of this Note briefly considers the function of the mens rea element in criminal statutes and the congressional vision for the role of the "knowledge" term in 18 U.S.C. § 2252. Part III outlines how developments in computer technology have created new pathways through which individuals can inadvertently receive child pornography. In light of these new possible scenarios of innocent receipt and possession, Part IV evaluates how federal courts have analyzed evidence of knowledge presented in child pornography prosecutions. Part V argues that courts' use of higher evidentiary standards for knowledge is supported by the standards' practical efficacy and their alignment with the purposes of the statute and the role of the judiciary. Part VI concludes.

II. THE "KNOWLEDGE" ELEMENT OF 18 U.S.C. § 2252

Federal courts have long required almost all criminal statutes defining offenses to include a mens rea term.[6] The inclusion of a mens rea element helps to sort cases that span a wide range of human behavior and to provide some form of moral evaluation for different individuals and their actions.[7] The Supreme Court considers this func-

[5] This understanding is also consistent with the widespread practice of legislative delegation of interpretive authority to courts as a means of allowing for the continued evolution of criminal statutes. *See, e.g.*, Dan M. Kahan, *Lenity and Federal Common Law Crimes*, 1994 SUP. CT. REV. 345, 347 ("The historic underenforcement of lenity . . . reflects the existence of another largely unacknowledged, but nonetheless well established, rule of federal criminal law: that Congress may *delegate* criminal lawmaking power to courts."); *see also* Martin R. Gardner, *The Mens Rea Enigma: Observations on the Role of Motive in the Criminal Law Past and Present*, 1993 UTAH L. REV. 635, 743 (discussing the relative merits of having legislatures and courts make adjustments to criminal laws). Professor Peter Henning argues that *United States v. X-Citement Video, Inc.*, 513 U.S. 64 (1994), which rejected the "natural grammatical reading" of the statute's mens rea term, encourages lower courts to stretch the language of statutes to achieve desired results. Peter J. Henning, *Foreword: Statutory Interpretation and the Federalization of Criminal Law*, 86 J. CRIM. L. & CRIMINOLOGY 1167, 1173 (1996) (quoting *X-Citement Video*, 513 U.S. at 68). Henning also asserts that stretching statutory language may create "greater imprecision by the legislature, since the courts will not respect the language anyway, and inconsistent results among different circuit courts and between states." *Id.* at 1170. The adjustments courts make when heightening the mens rea element through sufficiency of the evidence review, however, do not engage in such stretching of the structure of the text, but rather define the mens rea term by deciding what type of evidence is relevant.

[6] Christina Egan, *Level of Scienter Required for Child Pornography Distributors: The Supreme Court's Interpretation of "Knowingly" in 18 U.S.C. § 2252*, 86 J. CRIM. L. & CRIMINOLOGY 1341, 1355 (1996) (citing United States v. U.S. Gypsum Co., 438 U.S. 422, 437 (1978)).

[7] *See* Richard C. Boldt, *The Construction of Responsibility in the Criminal Law*, 140 U. PA. L. REV. 2245, 2280 (1992); *see also* Craig S. Lerner & Moin A. Yahya, *"Left Behind" After Sar-*

tion of mens rea so important that it may read a state-of-mind component into a criminal statute that lacks an express mens rea term.[8] The Court has also recognized that the mens rea determination is a question of fact, leaving to the factfinder the responsibility of evaluating whether the defendant acted with the requisite intent.[9] The intent element of criminal offenses "serve[s] a key screening function in our criminal justice system. [It] prevent[s] the conviction, punishment, and social disgrace of those who had no intent to engage in any criminal activity, and therefore have shown no need for corrective action."[10]

This general motivation for requiring a mens rea component is reflected in the legislative history of the knowledge term of § 2252. Congress made its first direct effort to outlaw child pornography with the passage of the Protection of Children Against Sexual Exploitation Act of 1977.[11] The parts of the Act focusing on the trade in pornographic materials depicting children were codified at 18 U.S.C. § 2252.[12] With the rise of the use of personal computers in the late 1980s, Congress moved to expand § 2252's reach, and in 1988 it passed amendments that explicitly added the language "by any means including by computer" to § 2252(a).[13] As the federal child pornography law evolved over time, its core intent requirement — that individuals receive, transport, ship, distribute, or possess child pornography "knowingly" — remained the same.[14]

Congress originally intended the term "knowingly" to serve a sorting function, separating inadvertent recipients of illicit materials from the genuinely culpable. Concern that the statute might be overly broad and reach innocent behavior was raised in the course of congressional debate about extending the bill to criminalize not only production of child pornography, but also its sale and distribution.[15] Re-

---

banes-Oxley, 44 AM. CRIM. L. REV. 1383, 1384 (2007); Jeffrey S. Parker, *The Economics of Mens Rea*, 79 VA. L. REV. 741, 742 (1993).

[8] *See, e.g.*, Morissette v. United States, 342 U.S. 246, 263 (1952) ("We hold that mere omission from [the statute] of any mention of intent will not be construed as eliminating that element from the crimes denounced.").

[9] *Id.* at 274.

[10] Note, *Protective Cruelty:* State v. Yanez *and Strict Liability as to Age in Statutory Rape*, 5 ROGER WILLIAMS U. L. REV. 499, 501 (2000).

[11] Pub. L. No. 95-225, 92 Stat. 7 (1978).

[12] *See id.* § 2252. Specifically, 18 U.S.C. § 2252(a)(1) applied to transporting or shipping child pornography, while § 2252(a)(2) was aimed at individuals receiving or distributing materials. *Id.*

[13] Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, sec. 7511(b), 102 Stat. 4485, 4485 (codified as amended at 18 U.S.C. § 2252(a) (2006)).

[14] *Compare* Protection of Children Against Sexual Exploitation Act of 1977 § 2252, *with* Child Protection and Obscenity Enforcement Act of 1988, sec. 7511(b), *and* 18 U.S.C. § 2252 (2006).

[15] *See* 123 CONG. REC. 33,049 (1977).

sponding to fear that the statute might create a "trap for the unwary,"[16] Senator William Roth emphasized:

> This amendment, limited as it is by the phrase "knowingly," insures that only those sellers and distributors who are consciously and deliberately engaged in the marketing of child pornography and thereby are actively contributing to the maintenance of this form of child abuse are subject to prosecution under this amendment.[17]

The same scienter element applies to each offense enumerated in § 2252, suggesting that Congress believed that including the term "knowingly" would also prevent the prosecution and conviction of the "unwary" recipient or possessor of child pornography.

Federal courts have long recognized that Congress intended the "knowledge" element of § 2252 to distinguish among levels of culpability and protect individuals who received child pornography mistakenly.[18] The Supreme Court, in *United States v. X-Citement Video, Inc.*,[19] considered the congressional intent behind § 2252's mens rea requirement when it decided exactly what facts a defendant must "know" to be convicted under § 2252.[20] In deciding whether the knowledge element of § 2252 extended to the "use of a minor" language in § 2252(a)(1)(A) and (a)(2)(A),[21] the Supreme Court focused much of its discussion on construing the meaning of the word "knowingly" to reflect Congress's aim of separating culpable offenders from inadvertent recipients of child pornography.[22] In *X-Citement Video*, the Court rejected the "natural grammatical reading" of § 2252's intent term, which would have suggested that "knowingly" only modified the statute's verbs — "transports, ships, receives, distributes, or reproduces."[23] The Court was troubled by the results of adopting such a construction — to do so, the Court concluded, would draw distinctions among individuals along illogical axes.[24]

---

[16] *Id.* at 33,050 (statement of Sen. Percy) (stating his understanding that the inclusion of the intent term would make the statute operate "such that a distributor or seller would be culpable only if he or she acts 'knowingly'").

[17] *Id.* (statement of Sen. Roth); *see also* United States v. Edwards, 92 CR 884, 1993 WL 453461, at *5–6 (N.D. Ill. Nov. 4, 1993) (discussing congressional deliberations on the intent standard in § 2252).

[18] *See, e.g.*, United States v. Osborne, 935 F.2d 32, 34 n.2 (4th Cir. 1991) (indicating that the words "knowingly received" were "intended to protect persons who have received child pornography by mistake").

[19] 513 U.S. 62 (1994).

[20] *Id.* at 78.

[21] *Id.* at 68.

[22] *See, e.g.*, *id.* at 75–76.

[23] *Id.* at 68.

[24] *Id.* at 69 ("It would seem odd, to say the least, that Congress distinguished between someone who inadvertently dropped an item into the mail without realizing it, and someone who consciously placed the same item in the mail, but was nonetheless unconcerned about whether the person had any knowledge of the prohibited contents of the package.").

To identify a more satisfactory understanding of § 2252's intent element, the *X-Citement Video* Court surveyed its prior holdings on the proper construction of criminal intent terms. The Court noted that in *Morissette v. United States*,[25] for example, it had "used the background presumption of evil intent to conclude that the term 'knowingly' also required that the defendant have knowledge of the facts" that made otherwise innocent conduct criminal.[26] Turning to its decision in *Liparota v. United States*,[27] the Court noted that it had worried that a "broader reading" of the statutory text would cover too much innocent conduct.[28] Focusing on the role of statutory intent terms in distinguishing levels of culpability, the Court concluded that "the presumption in favor of a scienter requirement should apply to each of the statutory elements that criminalize otherwise innocent conduct."[29] Because legal innocence under the statute turned on the ages of the individuals in the images, the knowledge term applied to the ages of the children depicted in the pornographic images.[30]

Though the *X-Citement Video* decision only directly addressed one aspect of § 2252's mens rea element — whether a defendant must have knowledge of the age of the children in the images — the Court's elaboration on the *purpose* behind the law's mens rea term has provided guidance to courts struggling with broader interpretive questions relating to the "knowledge" standard. Lower federal courts have followed the Supreme Court's lead in reading the "knowledge" element as a means of sorting between innocent and culpable behavior,[31] even as the paradigmatic application of § 2252 shifted from the mailing of videotapes at issue in *X-Citement Video* to the exchange or possession of electronic images. Because the Court's holding in *X-Citement Video* did not resolve all interpretive issues, however, courts still possess substantial leeway in determining what evidence is sufficient to demonstrate the requisite level of knowledge with respect to each of the elements of the crime.

---

[25] 342 U.S. 246 (1952).

[26] *X-Citement Video*, 513 U.S. at 70 (citing *Morissette*, 342 U.S. at 271).

[27] 471 U.S. 419 (1985).

[28] *X-Citement Video*, 513 U.S. at 71 (citing *Liparota*, 471 U.S. at 426). The Court continued, "Imposing criminal liability on an unwitting food stamp recipient who purchased groceries at a store that inflated its prices to such purchasers struck the Court as beyond the intended reach of the statute." *Id.*

[29] *Id.* at 72.

[30] *Id.* at 66.

[31] *See, e.g.*, United States v. Romm, 455 F.3d 990, 1003 n.16 (9th Cir. 2006) ("In *X-Citement Video*, the Supreme Court held 18 U.S.C. § 2252 requires the government to prove the defendant's knowledge that the performer depicted is a minor because this is 'the crucial element separating legal innocence from wrongful conduct.'" (quoting *X-Citement Video*, 513 U.S. at 73)).

III. MEANS OF INNOCENT RECEIPT AND POSSESSION VIA COMPUTER

The ease of internet communication and the low cost of transmitting electronic files have created new ways for individuals to become unintentional recipients of child pornography, and these means of delivery bear little resemblance to the bricks-and-mortar exchanges that Congress envisioned when drafting the original statute in 1977.[32] There are at least three new ways in which individuals might become unintentional recipients of child pornography in computer-based transactions: through unsolicited "spam" e-mails, pop-up advertisements during legal internet searches, and viruses. Suppose an unintentional recipient acquires illegal material, notices its presence on the computer, and either does not know how to delete it or thinks he need not delete it so long as he does not view it. That recipient may "knowingly" possess the material, yet still be the type of "unwary" recipient that Congress intended to protect by including the knowledge standard in the statute. This Part briefly surveys the mechanics of the internet that have made the possibility of unwitting receipt increasingly salient in cases involving computer-based receipt and possession of child pornography.

Child pornography can easily be transferred among individuals in the form of electronic images sent as e-mail attachments. Although e-mails containing illicit images can be solicited by participating in certain online chat rooms or websites, a person could also receive e-mails that are entirely unsolicited.[33] Once an image is sent, the recipient's computer may be equipped with software that automatically downloads the e-mail's contents onto the computer's hard drive. The user can, of course, choose to delete or retain any e-mails — including illegal spam — that he receives. This feature of e-mail communication suggests that while unintentional receipt may occur, subsequent knowing possession only occurs if a recipient chooses not to delete the file.[34] In the course of evaluating probable cause to conduct a search of a defendant's computer in *United States v. Kelley*,[35] Judge Rymer, writing for the court, acknowledged "the possibility that these e-mails *could*

---

[32] *See* Debra D. Burke, *The Criminalization of Virtual Child Pornography: A Constitutional Question*, 34 HARV. J. ON LEGIS. 439, 439–40 (1997) ("[T]he growth of Internet usage has resulted in a proliferation of on-line child pornography."); *see also* Marty Rimm, *Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2000 Cities in Forty Countries, Provinces, and Territories*, 83 GEO. L.J. 1849, 1914 (1995) (describing study in which researchers found that child pornography was widely available through computer networks).

[33] Giannina Marin, Note, *Possession of Child Pornography: Should You Be Convicted When the Computer Cache Does the Saving for You?*, 60 FLA. L. REV. 1205, 1214 (2008).

[34] *See id.* at 1217–18.

[35] 482 F.3d 1047 (9th Cir. 2007).

have been spam,"[36] but she ultimately found it unlikely that spammers would distribute the kind of illegal material that Kelley received.[37] Judge Thomas, dissenting in *Kelley*, disagreed, citing to a string of sources indicating that spam messages can contain illegal child pornography or links to illegal sites.[38] Though federal judges have disagreed about the likelihood that individual defendants came to possess electronic images of child pornography through unsolicited spam e-mails, they have nonetheless recognized that spam is at least a possible source of such images.[39]

Personal computer web browsers have a "cache" function in which they store copies of webpages viewed by a user, creating a second way that users might accidentally possess child pornography.[40] Because a computer's cache has a limited capacity, files are automatically deleted through a "first in, first out" system.[41] As an alternative, users can manually delete files from the computer's cache[42] or use commercial software to remove the files.[43] Because web browsers automatically save cached files, a person need not take any affirmative step to acquire the files in order for them to be saved to his computer. Typically, because files are saved from websites that a computer user has viewed on his screen, people who possess images of child pornography in their computer cache have also sought out the websites that display the original images. But even accidental viewing of an illegal image can lead to caching,[44] giving rise to the possibility that a person can pos-

---

[36] *Id.* at 1053.

[37] *See id.* at 1054–55.

[38] *Id.* at 1055–56, 1056 n.3 (Thomas, J., dissenting).

[39] *See* United States v. Falso, 544 F.3d 110, 116 (2d Cir. 2008) ("The district court also considered and rejected Falso's claim that the presence of his e-mail address on the website might simply have been the product of a spam mailing list. While recognizing the proliferation of spam, the court explained that Agent Lyons's affidavit suggested 'something more' — namely, that 'it appear[ed] that someone with [Falso's] e-mail address . . . either gained access or attempted to gain access to the website.'" (alterations and omission in original) (quoting the district court's February 24, 2006 oral ruling); United States v. Terry, 522 F.3d 645, 650 (6th Cir. 2008) ("It is thus impossible to know the context in which the image was sent; Terry argues that he may have merely been replying to some unsolicited child pornography spam to request that no further such images be sent to him. Although this is theoretically possible, it is not enough for Terry simply to speculate about hypothetical 'false-positive' scenarios." (footnote omitted)).

[40] Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1229–30 (2004).

[41] *Id.* at 1231 (internal quotation marks omitted) (citing Brian D. Davison, *A Web Caching Primer*, 5 IEEE INTERNET COMPUTING, July/Aug. 2001, at 38, 39).

[42] *Id.* (citing Microsoft, How To Delete the Contents of the Temporary Internet Files Folder, http://support.microsoft.com/default.aspx?scid=kb;en-us;260897 (last visited May 15, 2009)).

[43] *Id.*

[44] *See id.* at 1268 (noting a possibility that images in the computer cache resulted from a "'pop-up' banner" while a defendant engaged in legal browsing, and concluding that "[p]rosecutorial discretion dictates that a defendant who has a cache full of legal, adult pornographic web-

sess child pornography — even knowingly, having seen the unsought image and realizing that his computer has saved it in the cache — without ever having had any intent or desire to do so. If an individual lacks the technological sophistication to remove files from his cache or to ensure their permanent deletion, he "knowingly possesses" electronic images of child pornography within at least one reading of § 2252(a)(4).

A third means of unintentionally acquiring child pornography arises when a computer becomes infected with a virus.[45] United States federal courts have considered this possibility, but they have been slow to find that a virus was responsible for procuring the images on which child pornography charges are based. For example, in *United States v. Miller*,[46] the court relied on expert testimony[47] to conclude that "a person may come to knowingly possess a computer file without ever knowingly receiving it."[48] The court articulated one way in which unknowing receipt could lead to knowing possession: "This could happen . . . if the person's computer is infected with a virus or 'spyware' software that surreptitiously installs advertising images. Thus, when a defendant is charged with downloading a computer file, the court must rigorously scrutinize whether there is sufficient evidence to establish the intent-element of the crime."[49]

Though the Third Circuit ultimately rejected Donald Miller's claim that a computer virus had automatically downloaded illicit files,[50] at least one plausible account of a virus that did just that has been reported. In 2003, a British man was acquitted of child pornography charges in Exeter Crown Court "after arguing that the material had been gathered without his knowledge by a rogue program created by hackers — a so-called Trojan horse — that had infected his PC, probably during innocent Internet surfing."[51] Mark Rasch, a former U.S. federal computer-crime prosecutor, expressed concern over the

---

sites, but one image of child pornography that he visited once (and perhaps even deleted from the cache), should not be charged").

[45] *See, e.g.*, John Schwartz, *Acquitted Man Says Virus Put Pornography on Computer*, N.Y. TIMES, Aug. 11, 2003, at C1; *see also* Mark Rasch, *The Giant Wooden Horse Did It!*, THE REGISTER, Jan. 20, 2004, http://theregister.co.uk/2004/01/20/the_giant_wooden_horse_did/.

[46] 527 F.3d 54 (3d Cir. 2008).

[47] *Id.* at 63 n.8 ("Both the government's expert . . . and the defendant's expert . . . acknowledged the possibility that child pornography could be unknowingly downloaded onto a hard drive as the result of a virus, or 'spyware.'").

[48] *Id.* at 63.

[49] *Id.* (footnotes omitted) (citing United States v. Kuchinski, 469 F.3d 853, 861–63 (9th Cir. 2006) (reversing sentence for knowing receipt of child pornography in the form of cache files where defendant had neither knowledge of nor access to the files); United States v. Romm, 455 F.3d 990, 997–1001 (9th Cir. 2006) (upholding knowing receipt conviction where defendant knew he could access cache files)).

[50] *Id.* at 69.

[51] Schwartz, *supra* note 45.

implications of the British case: "The scary thing is not that the defense might work . . . . The scary thing is that the defense might be right . . . . The nightmare scenario . . . is somebody might go to jail for something he didn't do because he was set up."[52] While adequate forensic examination of a suspected individual's computer *should* be able to determine whether a virus may have downloaded child pornography, the British case suggests that prosecutorial investigation and discretion in deciding which cases to bring may be imperfect mechanisms — on their own — for ensuring that only truly culpable individuals are charged and convicted in child pornography cases.[53]

IV. JUDICIAL CONSTRUCTION OF § 2252'S KNOWLEDGE TERM

The problem of determining what types and quantities of evidence provide a sufficient basis from which a jury can infer knowledge is not unique to computer-based child pornography cases. Questions of proof of mens rea likewise arose under § 2252 in bricks-and-mortar cases, and courts responded to them, as they do now to cases involving electronic images, by weighing circumstantial evidence.[54] But the distinctly intangible nature of electronic image files pushes courts to rely on different forms of evidence to show knowing receipt and possession.[55] This Part will survey the patterns that have emerged from courts' analysis of the evidence relevant to proving knowledge in computer-based child pornography cases.

A. Affirmative Actions

Juries and reviewing courts often treat affirmative actions aimed at obtaining or preserving child pornography as compelling evidence of knowing receipt and subsequent possession. In *United States v. Stulock*,[56] for example, the defendant was acquitted on a knowing possession charge that was based on images saved in the defendant's browser cache.[57] The circuit court noted the district court's explanation "that one cannot be guilty of possession for simply having viewed an image on a web site . . . without having *purposely saved or downloaded* the

---

[52] *Id.*

[53] *But see* Howard, *supra* note 40, at 1268–69 (suggesting that prosecutorial discretion is sufficient to negate problems raised by the possibility of unintentional receipt and subsequent possession of images cached after viewing pop-up ads); Schwartz, *supra* note 45 (citing Department of Justice official as saying that a prosecutor would scan a computer to see if a virus could be responsible for downloading illicit files).

[54] *See, e.g.*, United States v. Brown, 862 F.2d 1033, 1038 (3d Cir. 1988).

[55] *See, e.g.*, *Miller*, 527 F.3d at 63 (discussing difference between tangible objects and computer files in terms of evidence of knowing receipt inferred from possession).

[56] 308 F.3d 922 (8th Cir. 2002).

[57] *Id.* at 925.

image."[58] Similarly, in *United States v. Riccardi*,[59] the government presented testimony that the defendant had received several pornographic images — including some depicting minors — in a "zip file" that he later unzipped and saved on his hard drive.[60] Government testimony suggested that Riccardi had created the directory in which the images were saved and that Riccardi would have had to direct the images to that directory.[61] The court concluded that these actions constituted "affirmative steps to preserve the child pornography on his computer," which was indicative of knowing possession.[62]

B. Access to Storage Area

At least one court has identified the "defendant's knowledge of and ability to access the storage area for the images" as a factor relevant to determining whether the defendant received child pornography "knowingly."[63] The Third Circuit decision in *Miller* separated the act and knowledge elements of the crime of knowing receipt of child pornography when considering the sufficiency of the evidence presented at trial.[64] After concluding that there was substantial evidence that Miller downloaded child pornography, the court moved on to the "[m]ore difficult" question of whether Miller acted "knowingly."[65] The *Miller* decision cited *United States v. Romm*[66] and *United States v. Kuchinski*[67] for the proposition that a defendant's ability to access cache files is relevant to determining whether he received them "knowingly."[68] In *Romm*, the Ninth Circuit reasoned that because the evi-

---

[58] *Id.* (emphasis added).

[59] 258 F. Supp. 2d 1212 (D. Kan. 2003).

[60] *Id.* at 1224 (internal quotation marks omitted).

[61] *See id.*

[62] *Id.*

[63] United States v. Miller, 527 F.3d 54, 67 (3d Cir. 2008) (citing United States v. Kuchinski, 469 F.3d 853, 861–63 (9th Cir. 2006); United States v. Romm, 455 F.3d 990, 997–1001 (9th Cir. 2006)).

[64] *Id.* at 66–67.

[65] *Id.*

[66] 455 F.3d 990. The defendant in *Romm* conceded knowledge on appeal; he contested the sufficiency of the evidence only on the "receipt" and "possession" elements. *Id.* at 997. While aspects of the evidence relevant to receipt and possession may also have supported a jury finding that the defendant acted knowingly, the court in *Romm* did not directly address what evidence would have demonstrated knowledge.

[67] 469 F.3d 853. In *Kuchinski*, the Ninth Circuit drew an analogy to *Romm*, noting in its discussion that Stuart Romm had conceded knowledge on appeal. *Id.* at 862 (citing *Romm*, 455 F.3d at 997). The *Kuchinski* court went on to explain that its decision in *Romm* had relied upon a Tenth Circuit case in which the defendant had contested the possession element of the crime, but admitted that he knew that images displayed on his web browser were saved in his computer's cache. *Id.* at 862–63 (citing United States v. Tucker, 305 F.3d 1193, 1204 (10th Cir. 2002)).

[68] *Miller*, 527 F.3d at 67–68. The court's analysis of the evidence relevant to proving knowledge under § 2252 demonstrates the difficulty courts have had in marking a clear distinction between evidence of knowledge and that of receipt or possession. The Third Circuit's reliance on

dence showed that Stuart Romm could and did control images of child pornography while they were displayed on his computer screen, the jury could reasonably have concluded that he possessed the images in his computer cache.[69] The court further noted that "[c]oupled with Romm's conceded knowledge that the images were saved to his disk," the prosecution had offered sufficient evidence to prove each of the elements of knowing possession under § 2252.[70] Considering similar factors, in *Kuchinski* the court found it significant that the defendant did not know about the images that were saved in the form of cache files only.[71] The court went on to conclude, "Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession . . . . To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control."[72] These cases embody the reasonable supposition that a person who had a sophisticated knowledge of computer functions like caching not only knew that viewing images on his computer screen would lead to receipt and possession, because a copy would be saved to his hard drive, but was also more likely to have accessed and viewed the images after they were preserved in the cache.

C. Efforts To Cover Up Prohibited Content by Deletion

Taking steps to cover up traces of prohibited content is another facet of defendant behavior that courts have found relevant to proving intent. For example, in *United States v. Tucker*,[73] the defendant argued that he did not "knowingly" possess child pornography because images were stored automatically in his computer's cache and he deleted them when he discovered that they were stored there.[74] But the court concluded that Tucker's actions, not any independent function of his computer, had caused the images to be stored:

> Tucker volitionally reached out for them. This is not a case of ignorance, mistake or accident. . . . *The fact that Tucker repeatedly deleted his cache files after his multiple visits to sites offering child pornography evidences his scienter*; Tucker would not know to delete the files from his computer if he did not know that they were on his computer drive.[75]

Romm and *Kuchinski*, cases in which the main focus was on evidence of possession or receipt, rather than of knowledge, blurs the lines between the act and mens rea elements of the statute.

69 *Romm*, 455 F.3d at 1001.

70 *Id.*

71 *Kuchinski*, 469 F.3d at 862.

72 *Id.* at 863.

73 150 F. Supp. 2d 1263 (D. Utah 2001), *aff'd*, 305 F.3d 1193 (10th Cir. 2002).

74 *Id.* at 1268.

75 *Id.* at 1269 (emphasis added). The use of evidence of deletion to prove knowledge is not wholly uncontroversial:

The *Tucker* analysis mixes evidence of deletion with repeat behavior, a related category of evidence of knowledge that courts often consider.

The reasoning of *United States v. Bass*,[76] in which the Tenth Circuit found that a jury could have reasonably inferred that the defendant knew that child pornography was being automatically saved to the computer he was using,[77] echoes that of *Tucker*. Evidence at trial indicated that the defendant had used two software programs to try to remove child pornography from the computer, and he admitted that he had used the programs because he wanted to prevent his mother from seeing the images.[78] The Tenth Circuit analogized *Bass* to *Tucker*, concluding that in both cases there was sufficient evidence of knowing possession to support a conviction under § 2252(a)(4).[79]

D. Repeat Behavior

As an alternative to evidence of affirmative acts, access, or deletion, courts have found it reasonable for juries to infer knowledge from indications of repeat behavior by the defendant. In *United States v. Fabiano*,[80] the Tenth Circuit considered evidence that John Fabiano had visited a preteen chat room over a period of about five months before receiving the images for which he was charged. On several specific occasions when Fabiano was logged into the chat room, participants explicitly discussed trading pictures with one another, conversations that included reference to the age of the children depicted in the images. Even after the defendant requested and received images via e-mail, he continued to visit the preteen chat room, on occasion attempting to set up trades with other participants.[81] The court found that a reasonable juror could have concluded that Fabiano knowingly received and possessed the two images he obtained via e-mail.[82] Evidence of repeated interest in child pornography — here, ongoing visits to chat rooms in which child pornography was regularly offered for trade — was held sufficient to support a finding of knowing receipt or possession.[83] In another repeat-behavior scenario, the

---

> With respect to knowledge, the *Tucker I* court reasoned that a computer user, by deleting a cached file, has at the very least demonstrated her knowledge of that file and the cache generally. Although such knowledge appears self-evident — except in the case of accidental deletion — it is not clear that that level of knowledge is sufficient to meet the knowingly standard required by most statutes.

Howard, *supra* note 40, at 1258 (footnote omitted).

[76] 411 F.3d 1198 (10th Cir. 2005).

[77] *Id.* at 1202.

[78] *Id.*

[79] *Id.*

[80] 169 F.3d 1299 (10th Cir. 1999).

[81] *Id.* at 1302.

[82] *Id.* at 1305–06.

[83] *Id.* at 1306.

First Circuit in *United States v. Wilder*[84] found that there was evidence that the defendant had used internet newsgroups as a means of collecting child pornography, downloaded child pornography, and viewed and deleted it, *repeating the process many times*, which gave rise to a reasonable inference of knowledge.[85] The *Wilder* analysis ties affirmative action to repeat behavior, further illustrating how the evaluative categories used by courts intersect.

V. THE NEED FOR JUDICIAL ELABORATION ON THE STATUTE'S CONTENT

The fact that the evidence courts have used to support a finding of knowing action has primarily fallen into the few categories outlined above gives content to the otherwise potentially indefinite term "knowingly" and helps to clarify § 2252's reach. If courts are to implement the statute as Congress intended, however, it is necessary to ask whether they have developed evidentiary standards that adapt the intent term to effectively screen out unwitting and mistaken recipients. Given the recognizable shortcomings of some alternative means of defining the statute's terms with greater precision and the strength of the match between courts' evidentiary standards and the computer-based sources of innocent receipt that have recently arisen, judicial efforts to develop consistent standards for evaluating evidence used to prove the elements of § 2252 are a desirable development.

A. Insufficiency of Other Means of Defining the Statute's Content

Legislatures' inability to define crimes with adequate precision is demonstrated by § 2252's affirmative defense, which, though evidencing congressional intent to remove likely cases of innocent receipt from the field of behavior punishable under the statute, fails to reach a substantial number of possible cases of mistaken receipt. The affirmative defense may protect some innocent defendants, but many will find themselves without the defense's protection. Background constitutional principles — such as the overbreadth doctrine — may provide assistance to a set of defendants who admit that their behavior satisfies each of the elements of the statute but contest the validity of a statute that can encompass behavior they would characterize as "innocent use." This type of legal argument does not, however, address the claims of defendants who assert that their behavior should not be construed as sufficient evidence to establish the elements of the statute. Overbreadth challenges are thus another form of incomplete protection that captures the claims of only some potentially innocent recipients.

---

[84] 526 F.3d 1 (1st Cir. 2008).

[85] *Id.* at 8.

1. Statutory Affirmative Defense Provision. — Congress has recognized the imprecision of § 2252's language and its potential mismatch with the activities that Congress actually meant to criminalize. In response, Congress has incorporated into the statute an affirmative defense provision that attempts to redefine child pornography crimes with greater specificity and to limit the statute's potentially broad scope. The provision, however, may fail to capture some activity that Congress wanted to remove from the statute's reach, as it only applies when an individual possesses fewer than three images and promptly destroys them or reports them to law enforcement.[86]

The availability of the affirmative defense provision helps to insulate mistaken recipients from charges of knowing possession,[87] but the defense alone is probably insufficient to achieve the intended level of filtering. In *Commonwealth v. Dingle*,[88] a case prosecuted under Massachusetts state child pornography law, the court stated that possession of a single image can constitute a violation of the state's statute.[89] Prosecutorial discretion may be one tool that helps to fill the gap left by the limitations of the affirmative defense, but the sentiment expressed in *Dingle* persists in the background. Even if it is not likely to happen frequently, prosecutors *can* charge someone with a violation of a child pornography statute on the basis of the receipt or possession of a *single image*. Moreover, if someone is sent an unsolicited e-mail attachment in the form of a .zip file and downloads the attachment to his hard drive, the file could easily contain more than three electronic images of child pornography, leaving the recipient without recourse to the affirmative defense. Given the ease with which individuals can send and receive large numbers of digital files, § 2252(c)'s affirmative defense alone may not adequately account for sources of potential passive receipt such as spam, pop-ups, and viruses.

Though Congress clearly intended to provide some means of separating levels of culpability when it created the affirmative defense provision, questions about the desirability[90] and effectiveness[91] of the af-

---

[86] 18 U.S.C. § 2252(c) (2006).

[87] Because of the aforementioned distinction between unintentional but knowing receipt and subsequent knowing possession, the fact that the affirmative defense provision applies only to possession should not undermine its effectiveness as a means of preventing the conviction of unintentional recipients who fall within its parameters.

[88] 898 N.E.2d 1 (Mass. App. Ct. 2008).

[89] *Id.* at 9.

[90] *See, e.g.*, United States v. Polizzi, 549 F. Supp. 2d 308, 342 (E.D.N.Y. 2008) ("The statute itself recognizes that it may constitute a lurking trap for the innocent; it includes a limited 'safe harbor' provision, but one that is insufficient to comport with due process requirements." (citing 18 U.S.C. § 2252(c))).

[91] *See, e.g.*, David T. Cox, *Litigating Child Pornography and Obscenity Cases in the Internet Age*, J. TECH. L. & POL'Y, Summer 1999, at para. 33, http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html.

firmative defense have been raised. For example, an "innocent interloper" is not necessarily protected by the affirmative defense; accidentally visiting a child pornography website may cause the computer cache to store several images, and the computer user may not know how to access and delete those cached images so as to comply with the affirmative defense requirements.[92] Law enforcement officials may also come into contact with illegal files in the process of investigating child pornography cases, and if more than three images are involved, these officials could be charged and find themselves without the benefit of the affirmative defense.[93] Many more mistakenly or innocently received or possessed images may fall outside the parameters of § 2252(c).[94] The affirmative defense provision is thus an incomplete means by which to ensure adequate sorting. Even where Congress makes a good faith effort to define crimes with greater precision, it may have difficulty matching the revised language of the statute to the exact factual circumstances to which it does or does not want the provision to apply.

2. Overbreadth Challenges. — Of course, the work of calibrating the terms of federal statutes need not be accomplished by courts through adjusted evidentiary standards alone. If the language of the statute does not describe the proscribed conduct with sufficient specificity, or if the statute is worded so as to capture a large range of innocent behavior, the statute may be challenged on overbreadth grounds. Such challenges have been leveled at § 2252, but courts have proven unreceptive to facial claims of overbreadth. For example, addressing an overbreadth and vagueness claim, one court concluded that the absence of an explicit exception for materials with "serious literary, artistic, scientific, or educational value" did not render the statute unconstitutionally overbroad.[95] Instead, the availability of an as-applied constitutional challenge was held sufficient to prevent the wholesale invalidation of the statute.[96] Similarly, the Fourth Circuit rejected a journalist's claim that the First Amendment protected his use of child pornography because his was a "'work of educational, medical or artistic value,' to 'create a work of academic, educational or political significance,' or 'a work of educational, literary, and political value,' and for other 'legitimate use[s],' including 'journalistic use[s].'"[97]

---

[92] *Id.*

[93] *See id.*

[94] *See id.*

[95] United States v. Lamb, 945 F. Supp. 441, 449–50 (N.D.N.Y. 1996).

[96] *Id.*

[97] United States v. Matthews, 209 F.3d 338, 344 (4th Cir. 2000) (alterations in original); *see also* Stanley v. United States, 932 F. Supp. 418, 421 (E.D.N.Y. 1996) ("On its face, the statute does not exclude materials which have serious literary, scientific, or educational value from forfeiture. It also appears that Congress did not intend to exempt such materials . . . . Legislative history of

Ultimately, though the possibility of an as-applied challenge on First Amendment grounds remains open, courts have proved unreceptive to "innocent use" exceptions to § 2252 where defendants knowingly received or possessed illegal child pornography. This type of challenge is, however, of a different nature than the question that courts have confronted when calibrating the level of evidence required to prove the elements laid out in § 2252. Courts evaluating the evidence used to prove the elements of a crime determine whether each element has been sufficiently established; courts addressing overbreadth claims instead decide whether, when all elements of the statute have been proven, the defendant should nonetheless go unpunished for his behavior. Because of this distinction, even if courts were receptive to overbreadth challenges, this mechanism alone would not sufficiently limit the statute's scope.

B. Match Between Evidentiary Standards and Inadvertent Recipients

The evidentiary standards described in Part IV, by contrast, add content to the meaning of the statutory text in a way that better captures the behavior that Congress meant to criminalize. Together, the mechanisms of evidentiary review developed by courts in computer-based federal child pornography cases help to protect defendants who may have been the mistaken or unwitting recipients of illicit materials delivered by spam, pop-ups, or viruses.

1. Spam. — When considering the evidence relevant to § 2252's knowledge element, courts rely heavily on measures that evaluate a defendant's affirmative actions to obtain, preserve, or dispose of child pornography. In a case in which child pornography has been received as spam e-mail, these models account for the most likely case of truly innocent receipt — receiving an e-mail without any prior contact with websites, chat rooms, or other forums in which trading in child pornography is discussed or arranged.[98] Someone who has received child pornography in this way and genuinely does not want it or intend to make use of it is unlikely to manipulate the images to demonstrate ongoing interaction beyond the step of acquisition.

The repeat behavior model also accounts for some cases in which receipt is most likely to be mistaken or unsolicited — those in which an individual receives a single e-mail with an illegal attachment. It

---

the Child Protective Act reveals that Congress rejected a proposed affirmative defense for serious literary, artistic, scientific, social, or educational value to prosecution under the child pornography laws." (footnote omitted) (citing 18 U.S.C. § 2251 et seq. (2006); H.R. REP. NO. 98-536, at 12 (1983), *reprinted in* 1984 U.S.C.C.A.N. 492, 503)).

[98] See Recent Case, 121 HARV. L. REV. 1261 (2008), for an argument that e-mail-based evidence should be evaluated for reciprocity.

does not account, however, for the possibility that a person's e-mail address could be introduced to a mailing list that regularly distributes illegal materials, which could generate multiple e-mails containing numerous illegal images that were not knowingly received. These images may qualify under some definitions of "knowing possession" if a recipient fails to delete them, even if he does not access or try to view them. Courts have typically addressed "spam" arguments when evaluating the sufficiency of affidavits to support a finding of probable cause to conduct a search.[99] The means of analysis they have employed, however, are not dramatically different from those with which judges review evidence establishing the elements of the crime. In *Kelley*, for example, the Ninth Circuit noted that the defendant had received the same type of child pornography in two separate e-mail accounts, adding up to a total of nine images.[100] "As a matter of practical, common sense," the court reasoned, "this is unlikely to occur without prior communication or connection."[101] Though repeat behavior may not account for all possible instances of mistaken receipt via spam e-mail, when it is taken together with evidence of affirmative steps to procure or subsequently access the image, courts are likely to be able to discern where genuine mistaken receipt and possession of electronic images delivered by e-mail has occurred.

2. Pop-up Caching. — The affirmative act and access models provide a meaningful, though possibly incomplete, screen for images acquired through caching of pop-up images. The match between this set of evidentiary tests and innocence is strongest where a mistaken recipient has no idea that his computer saved the files, never saw the website from which the images were cached, or does not have the sophistication to access files in his computer cache to remove or alter them. The Third Circuit in *Miller* considered "whether the defendant

---

[99] *See, e.g.*, United States v. Terry, 522 F.3d 645, 650 (6th Cir. 2008) ("Although we recognize that the government ultimately has the burden of demonstrating probable cause, absent *any* evidence that innocent persons frequently receive and reply to unsolicited child pornography spam (and in a way that would produce the computer traces in this case), this court cannot say that the magistrate judge arbitrarily exercised his discretion in issuing a search warrant for [the defendant's] home."); United States v. Kelley, 482 F.3d 1047, 1053 (9th Cir. 2007) (recognizing that the affidavit did not directly address the possibility that the e-mails were spam, but finding that [the defendant's] argument that they were spam was unpersuasive); *cf.* United States v. Hay, 231 F.3d 630, 634–36 (9th Cir. 2000) (holding that the district court's failure to consider spamming or automated bulk downloading theories, which might support the unlikely possibility that the suspect did not actually transmit nineteen images of child pornography himself, was not error in a probable cause determination). The fact that the spam issue surfaces when courts review search affidavits for probable cause might indicate that prosecutors rarely charge based on e-mail images that were likely the result of spamming alone. If so, this may be an area in which prosecutorial discretion is a particularly effective supplement to courts' evidentiary review in ensuring effective screening for culpability among potential defendants.

[100] 482 F.3d at 1053.

[101] *Id.*

had knowledge of and an ability to access the storage space for the images"[102] so as to satisfy the statute's mens rea term. The court found it "clear" that the defendant had access to the images.[103] Because the defendant had admitted to storing child pornography files to a disk, the court found:

> [T]he facts of this case are more akin to the facts of *Romm*, where the court found that the defendant's knowledge that he could access cache files supported the inference that he knowingly possessed the files, than to the facts of *Kuchinski*, where the court rejected this inference because the defendant was unaware of, "and concomitantly lack[ed] access to and control over the existence of the files."[104]

To further bolster the effectiveness of this type of evidentiary review, browser histories may help to determine the types of searches and web surfing in which individual defendants have engaged, corroborating a claim of accidental, unintentional pop-up receipt of the cached files.

Repeat behavior is also well suited to manage potential problems raised by cached images from pop-ups. Furthermore, this measure, when applied to cache files, does not suffer from the innocent distribution list possibility that applies to spam e-mail.[105] Because there is a level of computer user initiation, even if initially unintentional, in coming across illegal images during legal computer use, once an individual has accessed child pornography in the course of his online activities, he is likely, if genuinely uninterested in the material, to avoid sites that generate such images in the future. Though different, previously unvisited legal sites might produce images of child pornography on several distinct occasions, this seems less likely to happen to an innocent user than does the parallel spam situation[106] in which a single instance of a list obtaining a recipient's e-mail address can generate multiple instances of receipt of illegal images. Because internet users have the power to decide which sites they visit, they may possess greater control over the images that ultimately reside in their cache, over time, than do e-mail recipients, who can do little to prevent someone from sending them messages and images (though they retain the capacity to decline to view and/or to delete those images should they receive them).

---

[102] 527 F.3d 54, 68 (3d Cir. 2008).

[103] *Id.*

[104] *Id.* at 68 (alteration in original) (citations omitted) (quoting United States v. Kuchinski, 469 F.3d 853, 861–63 (9th Cir. 2006)) (citing United States v. Romm, 455 F.3d 990, 997–1001 (9th Cir. 2006)).

[105] *See supra* pp. 2221–22.

[106] It seems likely, however, that child pornography pop-ups are most often associated with sites that display things like legal adult pornography. An individual who regularly searches for certain types of otherwise legal material therefore may be more susceptible to repeat exposure to illegal images in pop-up advertisements than a person with different internet use practices.

3. Viruses. — Because it would be highly unusual for a user to affirmatively try to obtain a virus, the affirmative act evidentiary standard likely helps to screen for innocent receipt and possession. Of course, certain online activities may make one more likely to obtain a virus that collects child pornography, but because viruses are *intended* to be malicious, it is reasonable to believe that they may be packaged through otherwise legal online materials or as spam e-mail attachments. A virus recipient, like a spam or pop-up cache recipient, has the opportunity to access and manipulate the images once they are transferred to his computer. But courts have looked to concrete actions to determine whether there is adequate evidence of knowledge; the mere possibility of accessing the images is not enough. In *Miller*, the Third Circuit recognized that knowing receipt was not a prerequisite of knowing possession, particularly if the image was obtained while a computer was infected with a virus.[107] It is through additional steps to access the image that knowing possession may be established.

The repeat behavior model of evidence evaluation can help courts address the possibility that a user has obtained child pornography unintentionally via a virus, but only if used appropriately. Courts should look not to whether multiple images have appeared on a user's computer during a concrete period of time when the computer was infected, but to whether images have been obtained on several separate occasions over time. A virus can, for example, persistently download images,[108] but it seems unlikely that an individual would obtain viruses that collect child pornography on multiple separate occasions.[109] By isolating the time frame in which the user claims his computer was infected, courts can determine if there are other periods in which images were transferred to the computer.[110]

* * *

Though the above discussion recognizes that courts have not perfectly adapted § 2252 to computer-based information exchange, some combination of the above methods of evaluating the evidence used to establish the elements of the crime captures many likely instances of mistaken receipt of child pornography. The description of cases above emphasizes that the benchmarks often work together to reinforce the strength of the inference of knowledge. Recognizing the difficulty of

---

[107] 527 F.3d at 63.

[108] *See supra* pp. 2213–14.

[109] This is not, of course, impossible, particularly if an individual is the intentional target of a virus sent to him via e-mail.

[110] Significantly, this situation demonstrates the important role played by computer forensic experts in sorting evidence related to computerized transactions and electronic files; this type of technological expertise can go a long way toward identifying the patterns of behavior in which a computer user engaged, illuminating the affirmative act, access, and repeat behavior scenarios for juries and reviewing judges.

developing a single rubric that adequately captures all of the circumstances relevant to culpability under the statute, courts have taken a multifaceted approach to defining the statute's practical meaning.

C. Judicial Elaboration on the Definition of Crimes Is Desirable

Even if courts have developed a reasonable approach to evaluating evidence in child pornography cases, one might argue that they are not ideally situated to recalibrate the meaning of the terms of federal statutes. Indeed, even some courts have hesitated to use evidence of knowledge as a means of calibrating § 2252 to screen out innocent conduct. For example, Judge Weinstein's opinion in *United States v. Polizzi*[111] took issue with courts' use of evidence of "non-operative" facts as the basis for inferring the "knowledge" required by the statute.[112] *Polizzi* suggested that by considering evidence of behaviors not explicitly referenced in the statute, courts are impermissibly altering the scope of the behavior that the statute prohibits: "Most courts have avoided the 'knowing' problem by looking to other evidence to infer knowledge — in effect, an unauthorized expansion of the statutes' 'operative' words."[113] *Polizzi* noted, for example, that seeking out child pornography, a factor considered in *Romm* and *Tucker*, "is not an element of the crime."[114] Evidence of repeated viewing is similarly not a congressionally articulated element of possession,[115] nor is evidence that the defendant was surprised by remnants of images of child pornography on his computer,[116] nor is storage of images.[117]

A fact need not be an element of the statute to be relevant to the mens rea determination; so long as it is reasonably probative of some element of the crime as articulated in the statute, it is a permissible factor for fact-finders to consider.[118] By the terms of the statute, no defendant can be convicted on the basis of these "non-operative" elements alone; the government must also prove beyond a reasonable

---

111 549 F. Supp. 2d 308 (E.D.N.Y. 2008).

112 *Id.* at 357.

113 *Id.*

114 *Id.* ("Whether a defendant sought the images should have made no difference in determining what were operative elements of the statute, though it may have had a bearing on discretionary aspects of the sentence.").

115 *Id.*

116 *Id.* at 357–58.

117 *Id.* at 358. The *Polizzi* court did note that storage might be relevant to the defendant's "lack of knowledge" defense, *id.*, which seems to create an internal contradiction given that *knowledge* is an element of the statute.

118 *See* United States v. MacPherson, 424 F.3d 183, 189 (2d Cir. 2005) ("The law . . . recognizes that the *mens rea* elements of knowledge and intent can often be proved through circumstantial evidence and the reasonable inferences drawn therefrom." (citing Ratzlaf v. United States, 510 U.S. 135, 149 n.19 (1994); United States v. Salameh, 152 F.3d 88, 143 (2d Cir. 1998); United States v. Nersesian, 824 F.2d 1294, 1314 (2d Cir. 1987))).

doubt that the defendant "received" or "possessed" the forbidden materials. Thus, courts can only sustain a conviction where all elements of the crime have been proven.

Legislative history and the Supreme Court's interpretation of how the language of § 2252 expresses congressional intent suggest that both Congress and the Court view § 2252's knowledge term as meaningfully separating culpable conduct from mistaken or accidental acquisition and retention of illicit materials.[119] But *Polizzi* stated that in order for the statute to continue to prevent mistaken receipt from leading to criminal culpability, the intent term should be revised to a heightened standard such as "willfully" or "intentionally."[120] This analysis evinces a perspective that prizes explicit congressional revision of statutes as the primary means through which statutory terms may be adapted to changed circumstances. Presumably this argument derives from concerns about offending separation of powers principles and undermining legislative supremacy in defining crimes.[121] Such an approach is ill-suited to the realm of child pornography in which rapidly evolving technology is at the center of the statute's application to facts in individual cases. Because technological changes can be hard to predict, a focus on legislative revision as the only appropriate means of adjusting federal statutes would burden Congress with the task of constantly evaluating trends in internet communication and their effects on the child pornography trade. Given limited legislative resources and Congress's less direct access to information about the facts of child pornography exchanges,[122] overreliance on legislative revision is likely to prove inefficient or to fall hopelessly behind the state of technology. Further, because child pornography crimes are among the most stigmatized offenses, legislators may prove reluctant to define these crimes with great specificity, for fear of adopting a statute that is perceived as potentially letting the guilty go free.[123] In light of the lack of immedi-

---

[119] The *Polizzi* court implied that the statute was not intended to criminalize accidental receipt. *See* 549 F. Supp. 2d. at 353.

[120] *Id.*

[121] For a discussion of how separation of powers principles should inform federal criminal law, see Kahan, *supra* note 1, at 470 ("What forms of behavior fall within the ambit of criminal fraud statutes . . . are the products of judicial invention. Such inventiveness, moreover, does not reflect a lawless usurpation of legislative prerogative; rather, it is a response to the deliberate incompleteness of the criminal statutes that Congress enacts. For this reason, federal criminal law, as a whole, is best conceptualized as a regime of delegated common law-making." (citing Kahan, *supra* note 5, at 370–89)).

[122] Congress has less access to such information because whereas courts confront the evolving fact patterns regularly in the course of deciding cases, the legislature does not do so in the course of its day-to-day work.

[123] For an example of a situation in which fear of letting potentially guilty offenders go free pushed Congress to adopt a more comprehensive standard that encompassed more possibly innocent behavior, see *United States v. Matthews*, 209 F.3d 338, 349–50 (4th Cir. 2000), which noted

ate incentives for congressional revision, federal courts' competent work of implicitly adjusting the statute's scope to better match the facts of present-day cases is a positive development.

One might argue that a better, clearer way for courts to help update the statute would be to apply the statutory terms literally, possibly resulting in the conviction of defendants whom Congress would not have intended the statute to reach and thus pushing Congress to make the necessary revisions explicit in the text of the statute. Although the greater clarity that might result from such a revision would be ideal, the potential for delay and the harm to defendants convicted in the course of such an interbranch signaling exercise advise against such an approach. Child pornography–related crimes are highly stigmatized offenses. Because of the social, as well as legal, harm that befalls defendants convicted under § 2252, courts should be cautious about the possibility of convicting individuals whose behavior legislative history and past Supreme Court interpretations suggest was not meant to fall within the statute's reach.

VI. CONCLUSION

The work that courts do to define crimes left indefinite by statutory language helps to improve the match between the behaviors that Congress intended to criminalize and those that are punished under the statute. If there is concern about the statute reaching too much innocent conduct, the calibration of the statutory elements by courts is one way to ensure that the statute continues to capture only culpable individuals, even as the facts from which § 2252 cases arise evolve over time. As technology has changed and the majority of child pornography is now traded through personal computers via the internet, courts have translated the elements of the statute so that they make sense in this new factual context. The standards courts have developed line up rather well with the new challenges presented by electronic transfer of images, preserving the intended sorting function of § 2252's "knowing" term. These standards also signal to prosecutors the types of evidence they must present to demonstrate the elements of the crime and secure convictions under § 2252 in federal court. In this way, courts work with prosecutors to ensure that the right cases get prosecuted and serve as a backstop protecting innocent defendants in the rare cases where receipt of child pornography was truly inadvertent.

---

that Congress chose to avoid a broad affirmative defense provision that would except innocent "use" from prosecution under § 2252.