PUBLIC SURVEILLANCE THROUGH PRIVATE EYES: THE CASE OF THE EARN IT ACT AND THE FOURTH AMENDMENT

*Joseph Zabel**

I. INTRODUCTION

The explosive growth of the Internet has brought far-reaching social and economic benefits. However, largely unrestrained by regulation, it has also become a salt lick for illicit activity. Many have attributed the mushrooming of internet criminality in the United States to Section 230 of the 1996 Communications Decency Act (CDA), which confers broad immunity on Interactive Computer Service Providers (ICSPs) for content published on their platforms.[1] Some commentators view Sections 230's protections as nearly impenetrable, such that ICSPs have little incentive to ferret out crime that does not threaten them or their consumers.[2]

Meanwhile, online activity has become so vast that it has, in many ways, outpaced the traditional surveillance power of the government to identify illicit activity. In 2012, Professor Paul Ohm presciently forecasted that our future will be one in which "the police [will] shift from . . . producer to consumer of surveillance data."[3] Professor Ohm's prediction may soon come to fruition. Law enforcement increasingly must harness the power of outsourced surveillance—largely conducted by private companies—to close the growing surveillance gap.[4]

As outsourced surveillance continues to displace traditional surveillance, the boundary between ICSPs' private surveillance and law enforcement's insourcing of those data is liable to erode. As the line continues to blur, warrantless outsourced surveillance begins to implicate the Fourth Amendment. As it stands, the Fourth Amendment addresses private surveillance only if the surveillance

* J.D., Stanford Law School; B.A., Stanford University.

1. *See generally* 47 U.S.C. § 230 (2018) (the term "interactive computer service" refers to information systems which enable computer "access by multiple users" to a computer server including entities like Facebook, Twitter, and Google).

2. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 2, 401, 406–07 (2017).

3. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1348 (2012).

4. Such outsourced surveillance is not without precedent. *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976), in which the government required private banks to maintain customers' records for law enforcement access.

was "deputized" by state officials (i.e., that it was effectively compelled by the government), otherwise the search does not warrant Fourth Amendment scrutiny.[5] However, the inquiry as to whether or not a private actor has been deputized has become far less straightforward as law enforcement consumes more and more data from private enterprises.

Such Fourth Amendment issues abound in the iterations of the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act). There have been two versions of the Bill proposed. The first would require the government to withhold Section 230 immunity from ICSPs that do not implement "best practices" to fight the proliferation of Child Sexual Abuse Material (CSAM) on their platforms, or adopt undefined "reasonable measures" to do the same.[6] Specifically, if ICSPs do not comply with the "best practices" or "reasonable measures" they are exposed to civil liability and state prosecution.[7] The "best practices" requirement would likely mimic predecessor online statutes,[8] and require ICSPs to surveil and root out CSAM on their platforms, as is made plain in the "Matters Addressed" section of the bill. The second amended version (the currently active one)—the product of a "manager's amendment"—proposes simply eliminating ICSPs' Section 230 immunity for CSAM.[9] It nevertheless still intends to suggest a best practices template to identify CSAM.[10]

A critical question then (under the original or the amended statute) is whether the EARN IT Act deputizes ICSPs as outsourced private surveillance agents, such as to lay the groundwork for a springing Fourth Amendment violation. In that vein, this article proceeds in the following manner. First, it provides a brief explanation of Section 230 and the EARN IT Act. It then discusses the Fourth Amendment implications of the Act: 1) whether either iteration of the Act deputizes ICSP surveillance; 2) if it does, to what extent do individuals retain a reasonable expectation of privacy with respect to the content they post on ICSPs?; and 3) finally, are the actions "encouraged" by the EARN IT Act otherwise reasonable under the "special needs" exception to the Fourth Amendment?

5. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115 (1984).

6. *See generally* EARN IT Act, S. 3398, 116th Cong. § 6 (2020). If an ICSP decided to go down the "reasonable measures" path it would have had to litigate the question of whether its measures are "reasonable" for the purposes of immunity.

7. *Id.*

8. The "Stop Enabling Sex Traffickers Act" and the "Allow States and Victims to Fight Online Sex Trafficking Act" (Pub. L. 115–164, § 5, 132 Stat. 1253 (2018)).

9. *See generally* S.3398 (2020).

10. *Id.* at § 4.

II. SECTION 230 AND THE EARN IT ACT

The "shield" of § 230 makes it effectively impossible to hold ICSPs (either as publishers or as providers) liable for illicit content created and posted by users therein.[11] Thus, ICSPs—by many accounts—lack strong incentives to surveil for such content.[12]

The EARN IT Act (in the context of CSAM) may reverse this incentive problem. Right now, in order to fight the proliferation of CSAM, many ICSPs voluntarily scan files in users' accounts.[13] ICSPs must then report any CSAM they find to the National Center for Missing and Exploited Children (NCMEC), an organization which reviews the reports before passing them on to law enforcement.[14] However, many ICSPs do not conduct such surveillance programs, and, at least to date, have not been held liable for their inaction.[15] The original EARN IT Act statute, by removing ICSP immunity for those who do not take adequate steps, would effectively punch a hole in the § 230 shield. The amended statute, perhaps in recognition of the potential Fourth Amendment issues implicated in the original EARN IT Act throws the shield out altogether. It would lessen the legal force and thus overall suasion of the Act by entirely eliminating the prospect of safe harbor for ICSPs that comply with the government's proposed best practices and thus the obvious incentives to adopt those practices.[16] It is unclear whether or not the Act's enforcement would shift based on whether an ICSP did decide to adopt the proposed best practices. At the same time, by removing Section 230 immunity, the amended statute allows state criminal and civil actions against providers under the various state laws that govern CSAM.[17]

It may also be that the difference between the original and amended statute is merely cosmetic. On the one hand, the incentive structure in the second version is less explicit. On the other hand, the incentives will certainly persist if how the Act is enforced is calibrated to whether ICSPs follow the now-precatory recommendations, or if the various state laws effectively compel searches.

11. 47 U.S.C. § 230(C) (2018) ("[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider").

12. *See* Citron and Wittes, *supra* note 2.

13. *See, e.g.*, United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (describing AOL's scans for CSAM).

14. 18 U.S.C. § 2258A(a) (2018) ("duty to report").

15. There may be some moral and even business/reputational incentives to scan for such material but that incentive is not uniform and may be cost-controlled.

16. *See generally* EARN IT Act, S. 3398, 116th Cong. (2020)

17. For example, under the amended statute EARN IT Act, ICSP immunity for state criminal and civil laws "regarding the advertising, promotion, presentation, distribution, or solicitation" of CSAM, is eliminated, leaving ICSP subject to the legal standards existing in every state—which could turn out to lower the thresholds for liability for ICSPs.

III. DEPUTIZING INTERACTIVE COMPUTER SERVICE PROVIDERS

The drafters of the Act knew that if ICSPs were *formally* compelled to surveil their users for illicit activity on the government's behalf, ICSPs would become state actors.[18] Such warrantless ICSP searches could then violate the Fourth Amendment's prohibition on unreasonable searches and seizures. Still, the Act's structure to some degree betrays its drafters' true intentions. Moreover, the so-called "state actor" doctrine is not limited to *explicit* compulsion; private actors can become state actors even "when a search is not required by law," if a law "so strongly encourages a private party to conduct a search that the search is not primarily the result of private initiative."[19] The question is whether either iteration of the EARN IT Act's "encouragement" is coercive enough.

The Supreme Court has not spoken clearly on this question. Nonetheless, two cases that mark the inner and outer bounds of outsourced surveillance are *United States v. Jacobsen* and *Skinner v. Railway Labor Executives' Association*.[20] In *Jacobsen,* employees of Federal Express (now FedEx) searched the contents of a broken package and found white powder inside, prompting them to "summon[] a [DEA] agent."[21] The Court held that the Fourth Amendment did not apply to the employees' search because the Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official."[22]

In *Skinner*, a group of railway trade unions mounted a challenge to Federal Railroad Administration ("FRA") regulations which *permitted* private railroad companies "to administer breath and urine tests to employees who violate[d] certain safety rules."[23] The Court held that these regulations, which did not "compel any testing by private railroads," but merely facilitated it, still converted these private companies into state actors, noting that "[t]he 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."[24] The FRA had "made plain not only its strong preference for testing, but also [the Government's] desire to share [in] the fruits" of those tests.[25]

Meanwhile, lower courts remain divided and thus, different tests have emerged. The Court of Appeals for the First Circuit, for example, considers under its deputizing inquiry: "[1] the extent of the government's role in instigating or participating in the search, [2] its intent and the degree of control it exercises over the search and the private party, and [3] the extent to which the private party

18. *See* TECHFREEDOM, THE EARN IT ACT: CONCERNS & RESPONSES, https://techfreedom.org/wp-content/uploads/2020/03/EARN-IT-Concerns-and-Responses-2-28.pdf (document prepared by the Act's drafters).

19. United States v. Stevenson, 727 F.3d 826, 829 (8th Cir. 2013).

20. 466 U.S. 109 (1984); 489 U.S. 602 (1989).

21. *Jacobsen*, 466 U.S. at 111.

22. *Id.* at 113.

23. *Skinner*, 489 U.S. at 606.

24. *Id.* at 614–15.

25. *Id.*

aims primarily to help the government or to serve its own interests."[26] Some courts have held even *systematic* private surveillance for the benefit of law enforcement not to constitute deputization. For example, the Fourth Circuit determined that a hacker who repeatedly searched private computers for CSAM to assist law enforcement was deemed not to be operating as a state actor because his actions were of his own volition.[27] Courts have also upheld the constitutionality of ICSPs voluntarily but programmatically "hashing" emails for CSAM.[28]

A. Original Statute

The original version of the EARN IT Act falls somewhere in between *Jacobsen* and *Skinner*. Of course, determining whether ICSPs are deputized by the EARN IT act is a factual inquiry dependent on what specifically the "best practices" turn out to be. Still, much can be gleaned from the structure of the Act itself. By creating the risk of criminal and civil sanction for ICSPs which do not comply with the government's surveillance requirements, the government produces strong indirect incentives to surveil for CSAM, and disincentives for those that might otherwise not.

Nonetheless, the government previously disclaimed that "[n]othing in this Act . . . shall be construed to require a provider . . . to search, screen, or scan for instances of online child sexual exploitation."[29] Courts have pointed to similar disclaimers to reinforce their conclusion that providers are *not* state actors for Fourth Amendment purposes.[30] However, a mere disclaimer as to the lack of explicit compulsion—here one that seems like empty boilerplate—is probably insufficient to establish that a private actor's surveillance has not been deputized.[31]

In fact, this version of the Act is effectively compulsory in a few ways. To the extent that the motivations of the drafters can be discerned, the Act appears engineered to strong-arm ICSPs into complying with the government's "best practices." The gestalt of severe liability ($150,000 per CSAM image/video and *unlimited* punitive damages), the sheer quantity of CSAM on the Internet, the

26. United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009). For the 10th Circuit test, *see* United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) ("In determining whether a search by a private person becomes a government search, the following two-part inquiry is utilized: '1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.'" (internal citation omitted)).

27. United States v. Jarrett, 338 F.3d 339, 345–46 (4th Cir. 2003), *cert. denied*, 540 U.S. 1185 (2004); *see also* United States v. Koenig, 856 F.2d 843, 848–50 (7th Cir. 1988) (FedEx employee who repeatedly searched packages and reported the results to law enforcement was not "deputized.").

28. *See, e.g.*, United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013); United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012); United States v. Wellman, 663 F.3d 224, 226 n.2 (4th Cir. 2011) ("A 'hash value' is an alphanumeric string [which]. . . identif[ies] an individual digital file as a kind of 'digital fingerprint.'").

29. EARN IT Act, S. 3398, 116th Cong. § 6 (2020).

30. *See, e.g.*, *Stevenson*, 727 F.3d at 830.

31. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614–15 (1989).

potential for state prosecution, threatens ICSPs not only with sanctions but actual existential penalties.[32]

On the other hand, ICSPs are not *inherently* government adjuncts. And the EARN IT Act raises Fourth Amendment concerns only if the government chooses to prescribe best practices that effectively require ICSPs to perform a search. Moreover, a court might rule formalistically but with some logical appeal that "stripping immunity for companies that refuse to search for illegal content is *not* the same thing as requiring them to do so."[33] Finally, at least for some larger companies, the potential liabilities are likely not great enough to railroad them into modifying their surveillance practices.

Further, discerning the underlying purpose of an ICSP search might prove challenging. ICSPs rarely operate with only one motivation. Some circuits have held that mixed motives: intent to assist law enforcement and a concurrent "legitimate independent motivation" do not warrant Fourth Amendment scrutiny.[34] In that case, a private search will be likely be subject to Fourth Amendment restrictions only where the conduct has as its primary "purpose the intention to elicit a benefit for the government in either its investigative or administrative capacities."[35]

Nonetheless, the benefit to the government seems fairly cut and dried: to influence ICSPs to conduct extensive private surveillance of their users in order to identify CSAM (which they then must report to law enforcement). Thus, it would be difficult to argue that an ICSP that changes its practices does so primarily "to serve its own interests"; if the government was involved "directly as a participant . . . or indirectly as an encourager" then the intent of the private actor was likely primarily in service of law enforcement.[36] And leveraging Section 230 immunity as the mechanism of "encouragement" may be a thinly-veiled mandate. As noted above, that the Act offers a nominal alternative (under the original statute, ICSPs could also obtain Section 230 protections by proving the "reasonableness" of their practices) may be a risk companies are not willing to take when they could be exposed to costly lawsuits and prosecutions under 18 U.S.C. § 2255.[37] Thus, in the likely scenario in which few ICSPs choose *not* to adopt the Act's recommended "best practices" the fact of there being an alternative may not meaningfully affect a court's "state actor" analysis.

32. 18 U.S.C. § 2255(a) (2018).

33. *See* The EARN IT Act: Concerns & Responses, *supra* note 18.

34. United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981).

35. United States v. Attson, 900 F.2d 1427, 1431 (9th Cir. 1990); United States v. Andrews, No. 1:12CR100-1, 2014 WL 1663369 (N.D. W. Va. Apr. 23, 2014).

36. United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009); *see, e.g.*, United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996). Admittedly, this could be a very close call, as a company for its own moral and business reputation issues might want to be on the lookout for this activity.

37. *See supra* note 32 and accompanying text.

B. Amended Statute

In the second iteration of the Act, the Government has certainly tempered some of the more conspicuous Fourth Amendment issues. Indeed, depending on how the Act would be enforced, they may have eliminated them. For example, with no *explicit* incentive structure, the Act looks more akin to how one would envision ICSP regulation in the state of nature (i.e., without the grant of explicit immunity). The hammer that the Government now wields of full criminal and/or civil liability is thus simultaneously more forceful in one way and less so in another. It is more so because ICSPs now have no ability to immunize themselves from the Government's reach, but it is also less so because ICPSs will have weaker incentives to actually adopt the Government's preferred approach given that there is no explicit mechanism to "earn" immunity.

Still, much of the deputizing analysis for the amended statute may turn more explicitly on application/enforcement. If the Government has reason to believe that its proposed best practices, which remain even in the amended statute, would be most effective at rooting out CSAM, it may look to selectively enforce the law on those ICSPs that choose to reject the Government's recommendations, effectively compelling the adoption of those practices as in the first iteration of the Act.[38] The question then is whether such influence would be sufficient for a court to find that compliance with the best practices is "not primarily the result of [the provider's] private initiative."[39] If it is, the deputizing problem created by the first version is not entirely fixed.

Moreover, the second iteration of the Act also removes any previous immunity ICSPs had from prosecution or civil liability under state CSAM laws.[40] As a practical matter, ICSPs will have to alter their surveillance practices to match what is required under the strictest state law, and are thus at the whim of any state law changes as well.[41] This could potentially open up enough balkanized liability for ICSPs such as to constitute a form of deputization, entirely divorced from the concerns regarding the best practices themselves. Further, under the amended bill, "states would be empowered to criminalize not only the transmission of illegal CSAM but also 'solicitation' and 'promotion' of these images. These prohibitions would extend beyond the illegal CSAM itself to encompass a broader and less clearly defined category of speech."[42] Thus, the potential for deputization exists fundamentally in two spheres: (1) the states themselves could very well deputize ICSPs; (2) leaving ICSPs subject to such potentially draconian and atomized liability may be coercive enough to constitute deputization on its own.

38. *See* Riana Pfefforkorn, *The EARN IT Act Threatens Our Online Freedoms. New Amendments Don't Fix It*, STANFORD CTR. FOR INTERNET & SOC'Y (July 6, 2020, 11:45 AM), http://cyberlaw.stanford.edu/blog/2020/07/earn-it-act-threatens-our-online-freedoms-new-amendments-don%E2%80%99t-fix-it.

39. *Id.* (citing United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013)).

40. EARN IT Act, S. 3398, 116th Cong. § 6 (2020).

41. *Id.*

42. *ACLU Letter of Opposition to EARN IT Act Manager's Amendment*, AMERICAN CIV. LIBERTIES UNION (July 1, 2020), https://www.aclu.org/letter/aclu-letter-opposition-earn-it-act-managers-amendment.

IV. DO CONTENT-PRODUCERS HAVE A REASONABLE EXPECTATION OF PRIVACY?

Even if ICSPs operate as government surveillance adjuncts under the EARN IT Act, the third-party doctrine presents an additional challenge to any argument that the Act violates the Fourth Amendment. The fundamental question turns on whether individuals truly have a reasonable expectation of privacy in the content they post on ICSPs.

Courts have yet to answer. Nonetheless, most communications on ICSPs are stored on privately-owned third-party servers or Internet Service Providers.[43] Further, when users sign up to use these ICSPs, they usually accept (at least in theory) the terms and conditions, which likely include that the ICSP stores user data and may use those data for other purposes. Thus, at least on its face, there would be no constitutional barrier to the government's warrantless acquisition of these data.

For a deeper dive, *United States v. Miller* provides a familiar analogy.[44] In *Miller*, the Court held that the Fourth Amendment does not prohibit the government from obtaining bank information revealed to a third party "even if the information is 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."[45] Importantly, the Court held that "this analysis is not changed by the mandate of the Bank Secrecy Act that records of depositors/transactions be maintained by banks."[46] In the context of the EARN IT Act, users are probably similarly ignorant of the scope of the use of their data, and there is an analogous kind of *quasi*-mandate the government imposes on ICSPs.

On the other hand, in *United States v. Warshak*, the Sixth Circuit held that there is a reasonable expectation of privacy in the content of emails *even* if those emails were transmitted to a third party.[47] Thus, if the expectation of privacy for content-posters on ICSPs is only diminished, reasonableness balancing still applies. Further, because the Stored Communications Act imposes a warrant requirement on law enforcement's access to e-mails stored for fewer than 180 days, the legislature may still envision a reasonable expectation of privacy in that content.[48]

Moreover, *United States v. Carpenter* may complicate things.[49] While individuals who use ICSPs have in many ways waived their rights to privacy on the platforms, this was also the case with respect to cell site records before *Carpenter*.[50] Nevertheless, the Court pared back the third-party doctrine (at least

43. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 15–16.

44. 425 U.S. 435 (1976).

45. *Id.* at 443.

46. *Id.*

47. 631 F.3d 266, 286–88 (6th Cir. 2010). Courts could extend this ruling to other forms of ICSP data.

48. 18 U.S.C. § 2703(a) (2018).

49. 138 S. Ct. 2206 (2018).

50. *Id.* at 2217–18.

with regard to cell phones) and held that certain phone records could not be obtained without a warrant under circumstances where the search is highly intrusive.[51] *Carpenter* suggests that the boundaries of the third-party doctrine in the face of new technology, such as ICSP content, are not settled. Indeed, the increasing public scrutiny that companies like Facebook face may accelerate forthcoming legal challenges should the EARN IT Act pass.

Importantly, the *Carpenter* inquiry will likely be highly dependent on what the "best practices" turn out to be. Nonetheless, the Act's "best practices" will likely include some form of hashing in order to surveil for CSAM. Hashing is far less invasive, and far more targeted than most other "searches."[52] Commentators have suggested that perhaps hashing should appropriately be treated more like a canine sniff because—like drug-sniffing dogs—hash searches can be "trained (that is, programmed)" so as to only reveal CSAM.[53] In effect, use of hashing is a more binary inquiry: revealing either CSAM or nothing at all. In *United States v. Place*, a canine sniff of closed luggage was held not to be a search because the sniff did not require opening or rummaging through luggage; such searches disclose only presence or absence of narcotics.[54] Hashing similarly, if programmed properly, might disclose only the presence or absence of CSAM, in which case a court might find the Act's outsourced surveillance scheme (performed without a warrant) to be sufficiently targeted so as not to violate the Fourth Amendment.

V. DO EARN IT ACT SEARCHES QUALIFY UNDER THE "SPECIAL NEEDS" DOCTRINE?

Even if a court were to determine that the Act deputizes ICSPs in the course of EARN IT Act-influenced private surveillance, and that the content surveilled is *not* covered under the third-party doctrine, there remains a question of whether such warrantless searches are otherwise reasonable. One final defense the government could mount is that EARN IT Act searches are still reasonable under the "special needs" doctrine.

Otherwise unreasonable searches are reasonable if they are conducted for some special need outside of traditional law enforcement purposes.[55] In such cases, a court will consider the "balance between the public interest and the in-

51. *Id.* at 2221.

52. Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 44–46 (2005).

53. *Id.*; Dennis Martin, Note, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 715.

54. 462 U.S. 696 (1983); *see also* United States v. Jacobsen, 466 U.S. 109, 123 (1984) (a field chemical test "that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy.").

55. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 351(1985) (Blackmun, J., concurring) (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").

dividual's right to personal security free from arbitrary interference by law officers."[56] However, in the case of ICSPs and CSAM, law enforcement might struggle to persuade a court that such outsourced surveillance would be performed for a purpose other than law enforcement. Unlike highway checkpoints for drunk driving, (which are justified based on the belief that even a single drunk driver presents a broad risk to all drivers on the road), surveilling for CSAM does not ensure the safety of all internet users.[57] Although the government could argue that prevention of CSAM on the internet is primarily a safety concern, the Court has rejected the argument that the mere presence of CSAM on the Internet constitutes a broad enough safety risk to justify such searches.[58]

VI. CONCLUSION

As critics increasingly contend that Section 230 was not written for the Internet of today,[59] legislators will carve out exceptions such as the EARN IT Act that compel the "gatekeepers" of the Internet to surveil for illicit content. Privacy advocates will mount legal challenges to these exceptions, and when they do, courts will have to balance the potent crime-solving benefits of such surveillance against the potential deputizing of ICSPs and privacy intrusions that may be caused by having immunity stripped away.

56. Brown v. Texas, 443 U.S. 47, 50 (1979).

57. Indianapolis v. Edmond, 531 U.S. 32, 39 (2000).

58. 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 harm does not necessarily follow from the speech.").

59. *See, e.g.*, Matthew G. Jeweler, *The Communications Decency Act of 1996: Why § 230 Is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 U. PITT. J. TECH. L. POL'Y 3 (2007).