Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse

Anirudh Krishna*

The online proliferation of child sexual abuse material (CSAM), commonly referred to as child pornography, is a problem of massive scale. The National Center for Missing and Exploited Children (NCMEC), a private nonprofit specially authorized by Congress to serve as the nation's clearinghouse for reports of CSAM imagery, works with law enforcement to locate perpetrators and victims of child sexual abuse. In 2019, NCMEC received over sixty-nine million reports of CSAM, many of them from tech platforms like Google and Facebook.

DOI: https://doi.org/10.15779/Z38KW57J9B.

* J.D. Candidate, UC Berkeley School of Law
Advisor: Dr. Alexa Koenig, Executive Director, Berkeley Law Human Rights Center; Lecturer-in-Residence, UC Berkeley School of Law.
Special Thanks: Erwin Chemerinsky, Dean, UC Berkeley School of Law; Dr. Hany Farid, Professor, UC Berkeley School of Information; Andrea Lampros, Associate Director, Berkeley Law Human Rights Center; and Rebecca Wexler, Professor, UC Berkeley School of Law.
I would also like to acknowledge the three anonymous content moderators who shared so many personal details with me, at great personal risk, in order to shed light on their jobs and working conditions.

The proliferation of CSAM online can, in part, be attributed to the under-regulation of tech platforms. While Silicon Valley giants like Facebook have devoted some resources to the problem, these efforts are limited and flawed. Considering both their resources and their direct role in spreading CSAM, tech companies—even large ones—do very little to proactively combat child sexual abuse. That is because the current legal framework requires very little of them. For example, tech companies do not actually have to look for CSAM; they are only required to report CSAM to NCMEC if they become aware of it. Even then, the contents of these reports are optional. Moreover, section 230 of the Communications Decency Act shields tech companies from most legal liability even when people use their services to distribute and store CSAM. This legal protection further disincentivizes companies from looking for CSAM or investing in technology that could improve existing efforts. It is this problem that the proposed EARN IT Act—the subject of this Note—aims to address.

The EARN IT Act would induce tech companies to actively help detect CSAM and enforce CSAM laws. The Act creates a Commission—appointed by Congress and chaired by the Attorney General—tasked with developing best practices for reducing the volume of CSAM hosted on tech company servers. The Commission's best practices would cover everything from content moderator training and tip line reporting to the use of government-approved photo-matching software and the contents of companies' own terms of service. While the Commission's recommendations would technically be voluntary, the Act strongly incentivizes compliance by stripping tech platforms of their section 230 protections, thereby exposing them to a flood of costly CSAM-related litigation. To avoid being sued, companies would effectively have no choice but to comply with the Commission's recommendations, endorsed by the Department of Justice, and work proactively to detect CSAM and prevent its spread online.

In this Note, I argue that the EARN IT Act (or similar legislation), despite its worthy goals, would implicate the Fourth Amendment in potentially troubling ways, raising important questions about the Fourth Amendment's applicability in the age of social media. While the Constitution normally does not apply to private entities, I argue that the Act would convert tech companies into government agents—active participants in law enforcement. Their searches of user photos and videos would therefore count as government action subject to the Fourth Amendment. I support this conclusion with Supreme Court precedent and recent case law, including a pathmarking opinion by then-Judge Neil Gorsuch. For context, I also include a detailed look at Facebook's current approach to CSAM, relying on original interviews with three Facebook content moderators and the leading computer scientist in the field. After concluding that the EARN IT Act would implicate the Fourth Amendment by coercing tech companies into conducting searches for CSAM on behalf of the government, I consider whether such searches would actually violate the Fourth Amendment. I identify two ways courts could approve of such searches: the "third-party doctrine," and by analogy to drug sniffing dogs. While I conclude that the EARN IT Act is likely constitutional, its scheme raises important constitutional questions and represents a major shift in our relationships with both tech companies and the federal government. I therefore suggest that Congress legislate on digital privacy more broadly.

The EARN IT Act has strong bipartisan support; if for some reason it does not pass, it is very likely that a similar bill will. President Joe Biden has repeatedly expressed his desire to strip tech companies of section 230 protections, and prominent Republicans and Democrats have echoed these sentiments. Indeed, President Trump signed a bill into law that targets section 230 in much the same way the EARN IT Act does, albeit with a focus on sex trafficking. Thus, this Note's analysis is relevant not just to the EARN IT Act, but to future bills aimed at CSAM and section 230.

INTRODUCTION

In 2012, Reddit—one of the most popular websites in the world[1]—issued this statement to its users:

> We have very few rules here on reddit; no spamming, no cheating, no personal info, nothing illegal, and no interfering the site's functions [*sic*]. **Today we are adding another rule: No suggestive or sexual content featuring minors.**
>
> > In the past, we have always dealt with content that might be child pornography along strict legal lines . . . and when warranted we made reports directly to the National Center for Missing and Exploited Children, who works directly with the FBI. When a situation is reported to us where a child might be abused or in danger, we make that report. Beyond these clear cut cases, there is a huge area of legally grey content . . . . We have changed our policy because interpreting the vague and debated legal guidelines on a case by case basis has become a massive distraction and risks reddit being pulled in to legal quagmire. . . .
>
> We will tirelessly defend the right to freely share information on reddit . . . even if it is offensive or discusses something that may be illegal. However, child pornography is a toxic and unique case for Internet communities, and we're protecting reddit's ability to operate by

1. Joshua Hardwick, *Top 100 Most Visited Websites by Search Traffic (2021)*, AHREFS BLOG (Jan. 1, 2021), https://ahrefs.com/blog/most-visited-websites/ [https://perma.cc/VDK9-BVGJ].

> removing this threat. We remain committed to protecting reddit as an open platform.[2]

As the statement illustrates, large tech companies like Reddit have several incentives to cleanse their servers of child sexual abuse material (CSAM), more commonly known as child pornography.[3] Legal liability, public relations, and user retention are the most obvious incentives. And yet, despite calling child pornography a "toxic and unique case for Internet communities," it took Reddit seven years after its founding to issue an actual rule pertaining to child pornography.[4] All the while, it tolerated content on threads like "r/jailbait" and "r/preteengirls."[5] Only after Reddit was publicly shamed by outraged users did it finally declare suggestive content relating to children against the rules.[6]

A similar story recently played out with Pornhub, the most popular pornography website in the world.[7] For years, the company turned a blind eye as unverified users uploaded videos featuring child abuse and underage sex.[8] Despite victims calling for Pornhub to change its policies, the website only acted in December 2020, after the *New York Times* published a widely shared and

---

2. u/reddit, *A Necessary Change in Policy*, REDDIT (Feb. 12, 2012), https://www.reddit.com/r/blog/comments/pmj7f/a_necessary_change_in_policy/ [https://perma.cc/4Z6Z-CDGM]. Reddit's most current content policy is available at *Reddit Content Policy*, REDDIT, INC., https://www.redditinc.com/policies/content-policy [https://perma.cc/E97A-XLZ3].

3. While the terms "child pornography" and "child sexual abuse material" are more or less interchangeable, I believe the latter term more accurately describes the imagery of concern without euphemizing the horrific nature of the material. Some members of Congress appear to agree: a less controversial portion of the proposed EARN IT Act (discussed at length *infra* Part I.B, and throughout this Note) would replace all instances of the term "child pornography" in the United States Code with the term "child sexual abuse material," with no change in meaning. S. 3398, 116th Cong. § 6 (2020).

"Child pornography" is defined in 18 U.S.C. § 2256(8) as follows:

> "[C]hild pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—
>
> A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
>
> B. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
>
> C. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

4. u/reddit, *A Necessary Change*, *supra* note 2; *see About: Reddit Founders*, REDDIT, INC., https://redditinc.com [https://perma.cc/3SPL-3MZF] (noting Reddit was founded in 2005).

5. *See* Brett Smiley, *In Policy Shift, Reddit Bans Child Pornography*, N.Y. MAG. INTELLIGENCER (Feb. 12, 2012), https://nymag.com/intelligencer/2012/02/policy-shift-reddit-bans-child-pornography.html [https://perma.cc/WT5Y-XECD].

6. *See id.*

7. Joel Khalili, *These Are the Most Popular Websites in the World – and They Might Just Surprise You*, TECHRADAR (July 20, 2020), https://www.techradar.com/news/porn-sites-attract-more-visitors-than-netflix-and-amazon-youll-never-guess-how-many [https://perma.cc/8ZYJ-83VL].

8. *See* Nicholas Kristof, *The Children of Pornhub*, N.Y. TIMES (Dec. 4, 2020), https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html [https://perma.cc/8CZJ-2T22].

scathing piece about the presence of CSAM in Pornhub's video library, prompting Visa and Mastercard to reconsider doing business with the site.[9] Pornhub responded by deleting videos from unverified users (over 70 percent of its content), thereby allowing only vetted material to remain on the site.[10]

At this point, the reader may rightly wonder how Reddit and Pornhub hosted illegal content for so long without any significant legal repercussions. Why did it take a public outcry for the companies to do the morally obvious? The answer is that tech companies enjoy massive legal protections. Yes, knowingly possessing CSAM is a federal crime,[11] and companies are required by law to report CSAM when they find it.[12] But the law does not actually require these companies to look for CSAM in the first place, allowing for much of it to go undetected by companies that simply are not looking.[13] What is more, section 230 of the Communications Decency Act immunizes tech companies from civil liability for content posted by their users; in other words, a victim of child abuse cannot sue Facebook for allowing users to share a video depicting the abuse.[14]

That is not to say that tech platforms do nothing to detect CSAM. Large, public facing tech giants like Facebook, Microsoft, and Google use a mix of content moderators and photo scanning software to detect CSAM. However, this Note examines Facebook's system to illustrate why these efforts do not adequately address the problem. Moreover, smaller, less public-facing companies may have minimal incentives to invest in CSAM detection methods when the law does not require them to.

Unfortunately, the existing legal framework and current efforts by tech companies have not been nearly enough to effectively combat the exponential spread of CSAM online. In 2019, over sixty-nine million online images of child abuse were reported in the United States,[15] up from forty-five million in 2018, one million in 2014, and just one hundred thousand in 2008.[16] Perhaps the reader

---

9. *Id.*; Jacob Kastrenakes, *Pornhub Just Removed Most of its Videos*, VERGE (Dec. 14, 2020), https://www.theverge.com/2020/12/14/22173858/pornhub-videos-removed-user-uploaded-visa-mastercard-verified [https://perma.cc/BXW7-U2JL].

10. Kastrenakes, *supra* note 9; Nicholas Kristof, *An Uplifting Update, on the Terrible World of Pornhub*, N.Y. Times (Dec. 9, 2020), https://www.nytimes.com/2020/12/09/opinion/pornhub-news-child-abuse.html [https://perma.cc/K6KY-KAD6].

11. 18 U.S.C. § 2252A.

12. *Id.*

13. *See id.* (only requiring reporting if a company has "actual knowledge" of the presence of CSAM).

14. *See generally* 47 U.S.C. § 230(c)–(e).

15. Kristof, *supra* note 8.

16. Michael H. Keller & Gabriel J.X. Dance, *The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES (Sept. 29, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html [https://perma.cc/AQ9G-2N2J].

It is important to note that the exponential increase in *imagery* of child abuse does not imply an exponential increase in child abuse itself. What then does explain the surge? "It's a combination of things," says Dr. Hany Farid, a computer scientist at University of California, Berkeley. Interview with Dr. Hany Farid, Professor, U.C. Berkeley Sch. of Info., in Berkeley, Cal. (Nov. 21, 2019) [hereinafter

imagines these images circulating on the "dark web," somewhere in the deep recesses of the internet. The truth is that they spread on some of the most popular services in the world—services created by Google, Facebook, Apple, Microsoft, Dropbox, and Snap, Inc. Most readers likely use their products daily. Some CSAM has echoed across the internet for years, constantly copied, downloaded, forwarded in email chains, shared in Facebook groups, or stored in cloud-based platforms like Google Drive, Dropbox, Microsoft OneDrive, or Apple's iPhotos.[17] Often, the victims in these older photos are alive, out in the real world, traumatized by their experiences, and terrified that images depicting their abuse will resurface.[18] Other CSAM is newer, depicting children who are still experiencing abuse and who are in danger in the present day.

The proliferation of CSAM online has become so uncontrollable that law enforcement officials have been forced to triage. One officer confessed to the *New York Times* that she was in the unthinkable position of deciding which investigations to prioritize based on the age of the child.[19] Moreover, the National Center for Missing and Exploited Children (NCMEC), the nation's clearinghouse for reports of CSAM, is underfunded, which undermines its ability to quickly process reports and forward them to law enforcement.[20]

Against this dire backdrop, Attorney General William Barr has called for a more aggressive approach to the CSAM problem and so-called Big Tech's power over the online ecosystem.[21] On March 5, 2020, a bipartisan group of six Democratic and four Republican senators, including the highly influential Senators Lindsey Graham (R) and Richard Blumenthal (D), introduced a bill addressing the issue. Dubbed the "Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020," or the EARN IT Act ("the Act"), the proposed law seeks to make tech platforms do more to detect and report the enormous amount of CSAM online.[22] It establishes a commission, to be chaired

---

Dr. Farid Interview 1]. Dr. Farid created PhotoDNA, the photo-matching tool that helps tech platforms detect child pornography. *Id.* "We are finding more child abuse imagery in part because we are looking harder. At the same time, technology has also made it easier to produce, duplicate, and share widely." *Id.* Thus, it is impossible to know exactly how much of the increase in reports comes from increased production of CSAM and how much comes from increased efforts to track it down. *Id.*

17. Michael H. Keller & Gabriel J.X. Dance, *Child Abusers Run Rampant as Tech Companies Look the Other Way*, N.Y. TIMES (Nov. 9, 2019), https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html [https://perma.cc/27JL-JHRM].

18. *Id.*

19. *See* Keller & Dance, *The Internet is Overrun with Images of Child Sexual Abuse*, *supra* note 16.

20. *Id.*

21. Tony Romm, *Congress, Justice Department Takes Aim at Tech, Hoping to Halt Spread of Child Sexual Exploitation Online*, WASH. POST (Mar. 3, 2020), https://www.washingtonpost.com/technology/2020/03/03/section-230-justice-department-congress/ [https://perma.cc/UZQ4-LGYF]; Lauren Hirsch & Lauren Feiner, *Attorney General Barr Defends Antitrust Law as Elizabeth Warren Looks to Reinvent It*, CNBC (Dec. 11, 2019), https://www.cnbc.com/2019/12/10/barr-defends-antitrust-law-as-warren-looks-to-reinvent-it.html [https://perma.cc/S2ZQ-NAS9].

22. S. 3398, 116th Cong. (2020).

by the Attorney General, tasked with developing a series of best practices that tech platforms ought to follow to combat the proliferation of CSAM.[23] In addition, it exposes those same companies to potentially staggering levels of liability by creating a large carve-out in section 230 of the Communications Decency Act (CDA), the law that broadly shields tech companies from liability for the speech of their users.[24] An amended version of the Act advanced out of the Senate Judiciary Committee and was introduced to the Senate as a whole in July 2020.[25] A nearly identical (and also bipartisan) bill was introduced in the House in September 2020.[26]

The Act has been widely criticized. While much of this criticism has focused on the First Amendment,[27] some commentators have suggested that the Act violates the Fourth Amendment as well.[28] This Note addresses the Fourth Amendment question in depth by combining doctrinal analysis with original reporting on how tech companies confront the CSAM problem today. It concludes that the Act is likely constitutional, but that it will force courts to radically reconsider the Fourth Amendment's operation in a digital context. The Act would deputize private tech companies into acting as government agents when they search user accounts for CSAM. Because the Fourth Amendment applies to the government or its agents,[29] searches by tech platforms under the Act would be subject to constitutional scrutiny. Even if the federal courts eventually conclude that the Act does not violate the Fourth Amendment, they will have to do so by answering a bevy of novel legal questions, including in what ways the federal government may compel tech companies to help it enforce the law. If the EARN IT Act turns out to be constitutional, the federal government could use it as a blueprint to enlist tech companies in all sorts of law enforcement efforts, perhaps in less morally clear-cut contexts or in more invasive ways. Thus, this Note is as much about the methodology employed in

23. *Id.* at § 3.

24. *Id.* at § 5.

25. Makena Kelly, *A Weakened Version of the EARN IT Act Advances out of Committee*, VERGE (July 2, 2020), https://www.theverge.com/2020/7/2/21311464/earn-it-act-section-230-child-abuse-imagery-facebook-youtube-lindsey-graham [https://perma.cc/JS2G-K3SE]; Alexandra S. Levine, *Decision Time for EARN IT on Judiciary*, POLITICO: MORNING TECH (July 2, 2020), https://www.politico.com/newsletters/morning-tech/2020/07/02/decision-time-for-earn-it-on-judiciary-788955 [https://perma.cc/3LL2-4V9J].

26. Dennis Fisher, *House Version of EARN IT Act Introduced*, DECIPHER (Oct. 2, 2020), https://duo.com/decipher/house-version-of-earn-it-act-introduced [https://perma.cc/74DN-M39Y].

27. *See, e.g.*, Joe Mullin, *The New EARN IT Bill Still Threatens Encryption and Free Speech*, ELEC. FRONTIER FOUND. (July 2, 2020), https://www.eff.org/deeplinks/2020/07/new-earn-it-bill-still-threatens-encryption-and-free-speech [https://perma.cc/24ZT-228V].

28. *See, e.g.*, Riana Pfefferkorn, *The EARN IT Act Is Unconstitutional: Fourth Amendment*, STAN. L. SCH. CTR. FOR INTERNET AND SOC'Y: BLOG (Mar. 10, 2020), http://cyberlaw.stanford.edu/blog/2020/03/earn-it-act-unconstitutional-fourth-amendment [https://perma.cc/M2TA-73RP].

29. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) ("The [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.").

the EARN IT Act as it is about the Act itself. After all, even if the EARN IT Act does not pass, similar legislation likely will.[30]

This Note is organized as follows. In Part I, I provide an overview of statutory law governing tech companies and their relationship to NCMEC and law enforcement in the CSAM context. Then, I introduce the EARN IT Act and its regulatory scheme. I explain how the proposed law would dramatically change the existing statutory framework and force tech platforms to take CSAM more seriously.

The goal of Part II is to provide useful context by illustrating how one of most well-resourced corporations in the world—Facebook—currently approaches the CSAM problem. Drawing on both public information and my own reporting, I show that even one of the most closely scrutinized companies in the world falls far short in its approach to the CSAM problem. Three current and former Facebook content moderators walked me through the process they used to detect CSAM—a process I discovered was scientifically invalid and potentially racially biased. I also spoke with Dr. Hany Farid, a computer scientist who developed the CSAM detection software used by Facebook, Microsoft, and others. Dr. Farid explained both the benefits and limits of his photo-matching software, including how it cannot currently be used to scan encrypted messages sent on apps like Facebook-owned WhatsApp. This enormous loophole means that a large swath of Facebook's users is simply never subjected to the full force of Facebook's CSAM detection efforts. Facebook's flawed approach to CSAM illustrates that, when left to their own devices, even large, public-facing tech giants do not do nearly enough to prevent the spread of CSAM on their services. The EARN IT Act is an attempt by the federal government to induce better behavior.

In Part III, I discuss the government agency tests and cases that I apply to the EARN IT Act in Part IV. I focus on a recent Tenth Circuit case, *United States v. Ackerman*, which held that NCMEC is a government entity for the purposes of the Fourth Amendment.[31] That case opened the door for increased Fourth Amendment scrutiny of the legal framework around CSAM and the actors within it.

In Part IV, I apply the government agency tests discussed in Part III to the EARN IT Act's methodology. I conclude that the EARN IT Act, or similar

---

30. Indeed, a law called SESTA/FOSTA, passed in 2018 to combat online sex trafficking, employs some of the same methods as the EARN IT Act, including a section 230 carve-out. *See* 47 U.S.C. § 230(e)(5) ("No effect on sex trafficking law"); *see also infra* note 94 (explaining SESTA/FOSTA and its fallout in more detail); Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom [https://perma.cc/7HV9-G8T7] (discussing the law's impact on free speech and sex work). Because of the nature of CSAM and other features of the bill, however, the EARN IT Act's effects on the Fourth Amendment will likely be different.

31. (*Ackerman II*), 831 F.3d 1292 (10th Cir. 2016).

legislation, would convert tech platforms into government agents for purposes of the Fourth Amendment.

In Part V, I consider the implications of courts' finding that tech companies are government agents under a law like the EARN IT Act. In particular, I analyze the constitutionality of a warrantless search for CSAM carried out by a tech platform acting as a government agent under the EARN IT Act. I develop two separate theories under which such a search may be constitutional—analogy to drug-sniffing dogs and the third-party doctrine—and lay out the enormously difficult questions arising as a consequence of such a finding of constitutionality. I end by suggesting that Congress address these questions through digital privacy legislation rather than leaving the states and courts to answer them alone.

I.
MAPPING THE LANDSCAPE

This Section lays out how CSAM is detected and what happens after it is. Starting with the big picture, this Section maps the close working relationship between tech platforms like Facebook and the NCMEC and introduces the statutes governing that relationship. Then, this Section examines the EARN IT Act and its effect on the relationship between tech companies, NCMEC, and the government.

A. The Statutory Framework

Acts relating to the sexual exploitation of children are prohibited by Title 18 Chapter 110 §§ 2251–2260A of the U.S. Code. Federal law criminalizes the knowing possession, distribution, production, viewing, or receiving of child pornography and exposes those convicted of child sexual exploitation crimes to severe penalties.[32] Additionally, § 2255 creates a civil cause of action in federal court for victims of child sexual exploitation. It authorizes punitive damages and awards attorney's fees to successful plaintiffs.[33] But tech platforms like Facebook, Twitter, Google, and Microsoft are exempt from civil suits related to child pornography due to another statute called the Communications Decency Act of 1996 (CDA).[34]

Section 230 of the CDA was passed both to promote innovation on the Internet and to help companies moderate their content without fear of legal

32. 18 U.S.C. §§ 2252–2252A. *See generally* 18 U.S.C. §§ 2251–2260A.

33. 18 U.S.C. § 2255(a).

34. *See* 47 U.S.C. § 230(c). *See generally* Casey Newton, *Everything You Need to Know About Section 230: The Most Important Law for Online Speech*, VERGE (Dec. 29, 2020), https://www.theverge.com/21273768/section-230-explained-internet-speech-law-definition-guide-free-moderation [https://perma.cc/WK46-2D7W] (explaining how section 230 protects tech companies from legal liability and describing various attempts to reform it).

liability flowing from the speech of their users.[35] In light of these twin aims, section 230 provides that an "interactive computer service" cannot be treated as the "speaker" of user-generated content—including defamatory posts or imagery containing child pornography—and therefore cannot be held civilly liable as a speaker for material posted to its site.[36] Not only does this provide a "safe haven for websites that want to provide a platform for controversial or political speech,"[37] but it is also enormously beneficial to tech platforms from a financial perspective.

Leading internet law scholar David Post once opined that "no other sentence in the U.S. Code . . . has been responsible for the creation of more value than [34 U.S.C. § 230(c)(1)]."[38] The Electronic Frontier Foundation calls it "the most influential law to protect the kind of innovation that allowed the Internet to thrive since 1996."[39] As one observer put it, "Without Section 230 protections, websites would essentially be forced to hedge resources against unforeseen lawsuits based on unpredictable activity on the part of their users."[40]

Additionally, in the absence of section 230 protections, tech platforms would have to rethink their relationship with their users. For example, the CEO of Automattic, which owns the popular blogging service Wordpress, told EFF that without section 230, Automattic would have to fundamentally change its business philosophy.[41] Instead of promoting free speech, it would have to err on the side of removing posts and might even be forced to internally adjudicate legal claims arising out of user speech, like defamation.[42]

But section 230 does not shield online service providers from all responsibility for illegal content posted by users. In 2008, Congress passed the PROTECT Our Children Act to create a reporting requirement for tech companies with "actual knowledge" of the presence of CSAM or child

---

35. *See* 47 U.S.C. § 230(b)(1); Jeff Kosseff, *The Gradual Erosion of the Law that Shaped the Internet: Section 230's Evolution over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1, 6–8 (2016); Newton, *supra* note 34.

36. 47 U.S.C. § 230(c). The statute defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id.* § 230(f)(2).

37. *CDA 230: The Most Important Law Protecting Internet Free Speech*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 [https://perma.cc/LMB9-Q63Z].

38. David Post, *A Bit of Internet History, or How Two Members of Congress Helped Create a Trillion or so Dollars of Value*, VOLOKH CONSPIRACY (Aug. 27, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/27/a-bit-of-internet-history-or-how-two-members-of-congress-helped-create-a-trillion-or-so-dollars-of-value/ [https://perma.cc/2BNW-J3JP].

39. *CDA 230*, *supra* note 37.

40. Romano, *supra* note 30.

41. *CDA § 230 Success Case: WordPress.com*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230/successes/wordpress [https://perma.cc/DFD6-BSDQ].

42. *See id.*; *see also* Romano, *supra* note 30 (describing how tech companies responded with self-censorship when Congress removed § 230 protections for content related to prostitution and sex work).

exploitation on their services.[43] For example, if one of Twitter's users reports an instance of child pornography to the company, Twitter is supposed to file a report with NCMEC in addition to following its own internal reporting procedures. Twitter would also be required to preserve the image.[44] NCMEC in turn would share that report with law enforcement.

In reality, however, the reporting burden on tech companies is relatively low. None of the reporting requirements in Section 2258A come into play if a provider does not have "actual knowledge" of child exploitation. Remarkably, even if it has knowledge of an "imminent" act of child sexual exploitation, it does not have to report because the statute makes reporting an "imminent" act optional.[45] Furthermore, the government does not mandate that providers look for CSAM, making it less likely that they will acquire "actual knowledge" of it.[46] Thus, while *finding* CSAM triggers reporting responsibilities, *looking* for it is completely voluntary. This means tech platforms have neither a business incentive to look for CSAM (higher administrative costs) nor a legal incentive (looking could trigger reporting requirements). For companies that are not public-facing or highly scrutinized, there is even less pressure to actively search for CSAM.

Even when a company finds CSAM and files a report with NCMEC, the contents of that report are at the "sole discretion" of the company.[47] Nevertheless, the statute suggests tech platforms include the following in their reports (paraphrased): information about the individual involved (like email address, IP address, payment information); information relating to when and where the CSAM was uploaded, transmitted, or received (including time stamps, IP addresses, zip codes, and area codes); the CSAM itself; and the complete communication containing the CSAM (like an entire email chain).[48] The optional, somewhat toothless nature of the reporting requirement is undoubtedly designed to avoid the Fourth Amendment government agency scrutiny this Note engages with in Parts III – V. The more discretion tech companies have, the less likely it is that their actions are a result of government compulsion or coercion.

NCMEC, in turn, is a private nonprofit organization that serves as the country's clearinghouse for CSAM reports.[49] It is the only private entity exempt

---

43. PROTECT Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (codified in relevant part at 18 U.S.C. § 2258A).

44. 18 U.S.C. § 2258A(h).

45. 18 U.S.C. § 2258A(a)(1)(A)(ii) (maintaining that a provider *may* report planned or imminent CSAM violations as described in § 2258A(a)(2)(B)).

46. *See generally* 18 U.S.C. §§ 2251–2260A (not requiring providers to actively search for CSAM).

47. 18 U.S.C. § 2258A(b).

48. 18 U.S.C. § 2258A(b)(1)–(5).

49. *About Us*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://missingkids.org/footer/about [https://perma.cc/KCJ5-ZK7E]; 34 U.S.C. § 11293(b)(1)(B) (authorizing funding for NCMEC as the "national resource center and information clearinghouse for missing and exploited children"); 18 U.S.C. § 2258A(c) (referring to NCMEC's "clearinghouse role").

from laws criminalizing the possession of child pornography.[50] While NCMEC was not created by the government, it works closely with law enforcement officials and has close ties to the government. Roughly 62 percent of its total revenue of over fifty million dollars comes from government contracts and grants.[51] The FBI and other federal law enforcement arms have offices at NCMEC's headquarters.[52] Furthermore, NCMEC's CyberTipline, the mechanism through which tech companies (and the general public) may report potential CSAM, is mandated and authorized by statute.[53] When NCMEC receives a report through the CyberTipline, it must share that report with law enforcement.[54] NCMEC's forensic analysts investigate suspected CSAM imagery to determine whether it actually constitutes CSAM and whether a child might be in danger. NCMEC's analysts help determine which cases to pursue and even give leads to local law enforcement officers to aid their investigations.[55]

It is difficult to overstate how critical NCMEC's work is to the U.S. government's efforts to catch predators and rescue missing or exploited children. To illustrate the critical role NCMEC plays, here are some of NCMEC's other federally funded activities:

34 U.S.C. § 11293(b)…	**Activity**
(A)(1)	Operate a 24-hour-toll-free hotline
(B)	Operate the national resource center and information clearinghouse for missing and exploited children
(E)	Provide technical assistance to law enforcement, state and local governments, NGOs, local education agencies, and the general public
(H)	Provide forensic and direct on-site technical assistance and consultation to families, law enforcement agencies, child-serving professionals, and NGOs in child abduction and exploitation cases

50. *See* 18 U.S.C. § 2258D ("Limited liability for NCMEC"); *see also Ackerman II*, 831 F.3d at 1297 (explaining NCMEC's special status). In Part III, I explain more about NCMEC's relationship with the government and why that led the court in *Ackerman II* to conclude that NCMEC acts as a government agent for Fourth Amendment purposes. Interestingly, Canada has a similar setup. The Canadian Centre for Child Protection is also a nonprofit organization that serves as the country's clearinghouse for CSAM. *See History*, CAN. CTR. FOR CHILD PROT., https://protectchildren.ca/en/about-us/history/ [https://perma.cc/XX5J-N5CJ].

51. NAT'L CTR. FOR MISSING & EXPLOITED CHILD., 2018 YEAR IN REVIEW 2, https://www.missingkids.org/content/dam/missingkids/pdfs/2018%20Year%20in%20Review-web.pdf [https://perma.cc/DVT9-T6NX].

52. *Ackerman II*, 831 F.3d at 1298 n.4 (citing to United States v. Keith, 980 F. Supp. 2d 33, 41 (D. Mass. 2013), and to publicly available information from the Department of Justice's Office of Juvenile Justice & Delinquency Prevention).

53. 34 U.S.C. § 11293(b)(1)(K).

54. 18 U.S.C. § 2258A(c).

55. Dr. Farid Interview 1, *supra* note 16.

(K)(i)-(iii)	Operate a CyberTipline available to anyone; make tip line reports available to law enforcement; provide a victim ID service; utilize emerging technology to provide additional assistance to families
(M)	Provide technical assistance to local law enforcement and others

As critical as NCMEC's role is in fighting online child exploitation, it is obvious that the group cannot be successful without tech companies' cooperation. NCMEC could not provide law enforcement with the level of support that it does without the massive amounts of data contained in the CyberTipline reports it receives from tech companies. Nor could NCMEC effectively implement public education programs without support from tech platforms, as those platforms provide some of the most efficient ways to spread knowledge. It is no surprise, then, that NCMEC's board includes representatives from companies as diverse as Facebook, Adobe, and The Pokémon Company.[56]

B. The EARN IT Act's Bludgeon

As described in Part I.A, the fundamental problem with CSAM detection and enforcement today is that tech companies have weak incentives to actually look for it.[57] While large companies like Facebook do proactively search for CSAM, their efforts are outdated, scientifically invalid, and generally do not do nearly enough to address the scale of the problem.[58] This gap has allowed the mass proliferation of CSAM described in the Introduction. But if the government mandated that private companies actively search their users' private accounts for CSAM, it would unequivocally implicate the Fourth Amendment.[59] To avoid this problem, the EARN IT Act attempts to walk a fine line: the Act is framed in permissive terms—meaning compliance is technically voluntary—but is clearly intended to induce tech companies to adopt a more proactive commitment to detecting and reporting CSAM violations. What is more, in addition to increasing the level of commitment to addressing CSAM violations, the Act also seeks to influence the methods tech companies use. For reasons described in Part IV, the Act fails at its attempt to avoid Fourth Amendment scrutiny, but to understand why, it is first necessary to understand how the law would operate.

56. *Leadership*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/footer/about/leadership [https://perma.cc/D3XK-H377].

57. *See supra* notes 32–48 and accompanying text.

58. *See infra* Part II for details on Facebook's scheme.

59. *See infra* Parts III–IV for a discussion about government agency jurisprudence and why this would be problematic.

1. The Commission

The EARN IT Act's first order of business is to establish the National Commission on Online Child Sexual Exploitation Prevention ("Commission").[60] The Commission's purpose is to "develop recommended best practices that [tech companies] may choose to implement to prevent, reduce, and respond to" the trafficking of children and the proliferation of CSAM.[61] The Commission would have the power to hold hearings and gather evidence to inform its recommendations.[62] The bill stresses that following these recommendations is optional.[63]

The Commission would contain nineteen members and be chaired and controlled by the U.S. Attorney General.[64] It would also include the Secretary of Homeland Security and the Chairman of the Federal Trade Commission (or their representatives).[65] The remaining sixteen members would be appointed by congressional leaders in both parties. These members must include four industry representatives; four members with law enforcement or prosecutorial experience; experts on constitutional law, privacy, cryptography, or data security; and survivors of child abuse or people with experience providing services to survivors.[66] The Commission would meet at the call of the Attorney General and submit its recommendations directly to the Attorney General.[67] Fourteen votes are required before the Commission can make a recommendation.[68] Recommendations would be published directly on the Department of Justice website and in the Federal Register, [69] and would be updated at least once every five years.[70]

So, where would the Commission focus its energy? In testimony given to the Senate Judiciary Committee in March of 2020, NCMEC supported the EARN IT Act and expressed its hope that the Commission would address the following areas:

1. lack of consistent practices and technology across the tech industry to combat the problem of CSAM;
2. companies' failure to implement best practices across all of

60. S. 3398, 116th Cong. § 3.
61. *Id.* § 3(b).
62. *Id.* § 3(i).
63. *Id.* § 3(b) (stating that companies "may choose to implement" the best practices); § 4(a)(1)(A) (same). The bill uses permissive language throughout. *See, e.g.*, § 7(a)(1)(B)(iii) (laying out formatting guidelines for content that providers "voluntarily" include in reports to NCMEC); § 8(2) (describing the preservation of CSAM for research purposes as voluntary). As described in Part III.A and Part IV, this permissive language is unlikely to substantially affect the Fourth Amendment analysis.
64. *Id.* §§ 3(c)(1), 3(f).
65. *Id.* § 3(c)(1)(B).
66. *Id.* § 3(c)(1)(C), 3(c)(2)(A)–(D).
67. *Id.* §§ 3(h), 4(a)(1)(A).
68. *Id.* § 4(a)(2).
69. *Id.* § 4(b).
70. *Id.* §§ 4(a)(5).

their platforms and services;

3. reliance on wholly voluntary measures to protect children from being enticed or groomed online for sexual abuse and to prevent images of their rape and sexual abuse from circulating online;
4. absence of incentives for tech companies to invest and engage in best practices to keep children safer online; and
5. denial of a child victim's right to their day in court against all parties, including tech companies, that have recklessly contributed to the child's revictimization when sexually abusive images are recirculated online.[71]

The EARN IT Act also lists issues that the Commission might address.[72] Because these issues are expansive, it is worth considering the topics they would address in their entirety (paraphrased): (A) preventing, identifying, and reporting CSAM and child sexual exploitation; (B) & (C) coordinating with nonprofit organizations to preserve CSAM and related user identification; (D) receiving and triaging CSAM reports from users; (E) implementing a standard rating and categorization system for CSAM; (F) training and supporting content moderators; (G) issuing reports and incorporating disclosures about efforts to combat CSAM into terms of service; (H) coordinating with other tech companies in voluntary CSAM-related initiatives; (I) introducing age restrictions to prevent exploitation; (J) offering parental control products on websites and social media; and (K) contractual and operational practices to ensure third parties, contractors, and affiliates comply with the best practices.[73]

Notice the variety of topics covered and how the best practices would cover nearly every aspect of a tech company's operations related to CSAM, including the prevention and reporting of CSAM, case triage, content moderator training, and even a company's contractual obligations with third parties.[74]

Recommendations on topic (A) might stress adoption of the photo-matching tool PhotoDNA[75] along with a standardized way of assembling reports of potential violations with law enforcement. Since current law already lists the types of information companies may choose to include in a report,[76] the Commission might seek to set a minimum standard or to be even more specific.[77]

---

71. *The EARN IT Act: Holding the Tech Industry Accountable in the Fight Against Online Child Sexual Exploitation: Hearing on S. 3398 Before the S. Comm. on the Judiciary*, 116th Cong. 5–6 (2020) (statement of John Shehan, Vice-President, Exploited Children Division National Center for Missing & Exploited Children).

72. S. 3398 § 4(a)(3).

73. *See id.*

74. *See id.*

75. *See infra* Part II.A (explaining PhotoDNA in detail).

76. *See* 18 U.S.C. § 2258A.

77. *See* S. 3398 § 7 (detailing additional content, such as location data, that providers may choose to include in reports to NCMEC and specifying that providers "shall" do their best to format those reports in a manner approved by Congress).

Recommendations on topics (E) and (F) could ask that companies do more to train and support content moderators. Today, content moderators are typically poorly supported, low-wage independent contractors forced to view some of the most horrific material on the internet.[78] The government has an interest in how well content moderators do their jobs because content moderators are often on the frontlines of finding potential predators and referring them to law enforcement. The better their training, support, and triage skills, the more effectively they serve the government's law enforcement needs.

Recommendations centered on (C) and (D) would likely standardize how companies preserve and triage CSAM reports. Indeed, the EARN IT Act goes so far as to allow tech companies to hold onto CSAM *indefinitely*, so long as they are using it to research and develop CSAM detection and prevention mechanisms.[79] In other words, activity that would blatantly violate CSAM laws[80] is excused as long as the tech platform helps the government.

The Commission would likely develop more detailed guidelines while also homogenizing how companies identify the most urgent cases for law enforcement—another activity in which the government has a direct interest.

Not all tech platforms would be held to the same standard. The Commission may recommend alternatives to its best practices that account for a provider's "size, type of product, and business model," including whether its services are made available to the public or to other businesses.[81] Still, the recommendations would affect any company operating online regardless of size.

2. The Section 230 Carve-Out

Of course, the Commission's recommendations would be optional,[82] but the bill strongly incentivizes companies to comply. Recall that section 230 operates by shielding internet platforms from liability for their users' actions. The EARN IT Act amends section 230 by adding a carve-out section called "No

78. *See generally* Casey Newton, *The Trauma Floor: The Secret Lives of Facebook Moderators in America*, VERGE (Feb. 25, 2019) [hereinafter *The Trauma Floor*], https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona [https://perma.cc/ZJ4D-PR3K]; Casey Newton, *Bodies in Seats: At Facebook's Worst-Performing Content Moderation Site in North America, One Contractor Has Died, and Others Say They Fear for Their Lives*, VERGE (June 19, 2019) [hereinafter *Bodies in Seats*], https://www.theverge.com/2019/6/19/18681845/facebook-moderator-interviews-video-trauma-ptsd-cognizant-tampa [https://perma.cc/C239-6UHK]; Elizabeth Dwoskin, Jeanne Whalen & Regine Cabato, *Content Moderators at YouTube, Facebook and Twitter See the Worst of the Web – and Suffer Silently*, WASH. POST (July 24, 2019), https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price [https://perma.cc/4WVC-HA5T]. See Part II for a detailed discussion of content moderators at Facebook based on my own reporting.

79. S. 3398, 116th Cong. § 8 (2020).

80. *See* 18 U.S.C. § 2252A.

81. S. 3398 § 4(a)(1)(B)(i).

82. *Id.* § 3.

Effect on Child Sexual Exploitation Law." [83] This amendment would strip tech companies of immensely valuable section 230 protections with respect to CSAM posted by their users; this would open the companies up to criminal and civil liability, including punitive damages, under state and federal law.[84] Given that Facebook removed 8.7 million images of CSAM in one quarter in 2018[85] and 11.6 million images between July and September of 2019,[86] the section 230 carve-out could lead to a staggering level of expensive and time-consuming litigation for tech companies, regardless of their ultimate guilt. Some critics of the Act fear that the carve-out would also put tech companies at the mercy of state governments.[87]

But all would not be lost. Without saying so explicitly, the Act provides a way out: the Commission and its recommended best practices (described in the previous section). Remember, the Commission's recommendations are not legally binding. But civil lawsuits unleashed upon tech companies by the carve-out would likely end up revolving around how hard they have tried to stop the spread of CSAM on their services. Since the Commission would be comprised of experts and industry representatives and be chaired by the Attorney General, its recommendations would play a huge role in defining what it means for tech companies to act reasonably with respect to CSAM. Thus, with one hand, the government exposes tech companies to a tsunami of potential lawsuits, and, with the other hand, it offers them a pre-approved list of steps they can take to avoid liability. Indeed, an earlier version of the Act explicitly stated that tech companies could "earn" back their section 230 protections by following the Commission's recommendations.[88] The current version leaves this only implied, but the spirit remains the same: if a company can show that it is following best practices laid out by the Commission, it will be much harder to prove in court that it acted irresponsibly with respect to CSAM.

The Senate's version of the Act takes another step to temper potential legal liability by allowing companies to continue to provide end-to-end encrypted services, like WhatsApp or Signal, even if those services are used to distribute CSAM.[89] This dynamic reveals the government's confidence that the EARN IT

---

83. *See id.* § 5.

84. *Id.*; *see* 18 U.S.C. §§ 2252–2252A, 2255. The EARN IT Act preserves the CDA's "Good Samaritan" protections, which shield a company from liability for actions taken in good faith to detect, remove, and report CSAM. S. 3398 § 5; *see* 47 U.S.C. § 230(c)(2) (CDA's Good Samaritan clause).

85. Press Release, Antigone Davis, Facebook, New Technology to Fight Child Exploitation (Oct. 24, 2018) [hereinafter Davis, Facebook Press Release], https://about.fb.com/news/2018/10/fighting-child-exploitation/ [https://perma.cc/HCB7-9GKT].

86. *Facebook Removes 11.6 Million Child Abuse Posts*, BBC NEWS (Nov. 13, 2019), https://www.bbc.com/news/technology-50404812 [https://perma.cc/N2ST-BXYT].

87. *See* Kelly, *supra* note 25.

88. Hence the name "EARN IT Act"! *See* S. 3398, 116th Cong. § 6 (as reported by S. Comm. on the Judiciary, Mar. 5, 2020).

89. S. 3398 § 5. This was in response to criticisms that the EARN IT Act is intended to be an attack on encryption. *See* Kelly, *supra* note 25.

Act can induce more participation by tech companies without the government having to mandate that participation.

As the reader can see, despite its insistence otherwise, the EARN IT Act would represent a major change for tech companies. It would all but force them to take an active and aggressive role in preventing, detecting, and reporting CSAM or face potentially crushing legal liability. As I discuss further in Part IV, this dynamic would result in tech companies engaging in government-induced searches of their own users, the benefits of which the government directly reaps.

3. Current Status and Outlook

In July 2020, the EARN IT Act passed out of the Senate Judiciary Committee and was placed on the legislative calendar.[90] A nearly identical bill was introduced in the House in September.[91] As we wait to see how Congress will ultimately vote, it is important to remember that this bill does not exist in a vacuum. Bipartisan calls for reform of the CSAM statutory framework have intensified in recent years. The PROTECT Our Children Act of 2008, which created the reporting requirement for tech companies that detect CSAM on their servers, was sponsored by none other than then-Senator Joe Biden.[92] Furthermore, section 230 of the CDA has become enormously controversial in recent years, both among politicians and academics. President Biden has been a vocal critic of section 230, telling the *New York Times* in 2019 that "Section 230 should be revoked[] immediately" because it allows tech companies to act irresponsibly.[93]

Conservatives have also called for reforming section 230 and have not been shy about threatening to strip tech companies of their protections. As recently as 2018, President Trump signed into law a bill commonly known as SESTA/FOSTA, which created a carve-out in section 230 for violations of sex trafficking law (though without an EARN-IT-style Commission).[94] And in 2020,

---

90. *See* S. 3398 – EARN IT Act of 2020, CONGRESS, https://www.congress.gov/bill/116th-congress/senate-bill/3398?q=%7B%22search%22%3A%5B%22s.+3398%22%5D%7D&r=1 [https://perma.cc/RDK3-8RLX].

91. H.R. 8454, 116th Cong. (2020).

92. PROTECT Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229 (listing Mr. Biden as the main sponsor of the bill).

93. Joe Biden, U.S. President, Interview with the N.Y. Times Editorial Board (Dec. 16, 2019), *in* N.Y. TIMES (Jan. 17, 2020), https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html [https://perma.cc/8BY2-QFK4].

94. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018); *see* 47 U.S.C. § 230(e)(5) ("No Effect on Sex Trafficking Law"). SESTA/FOSTA is aimed at protecting victims of sex trafficking and preventing sex workers from soliciting work online, though its critics have argued that the law has backfired by forcing sex workers underground and into dangerous situations. *See* Karol Markowicz, *Congress' Awful Anti-Sex-Trafficking Law Has Only Put Sex Workers in Danger and Wasted Taxpayer Money*, BUS. INSIDER (July 14, 2019), https://www.businessinsider.com/fosta-sesta-anti-sex-trafficking-law-has-been-failure-opinion-2019-7 [https://perma.cc/226D-MNPG]; *see also* S. 3165, 116th Cong. (2020) (a bill sponsored by Senator Elizabeth Warren to study the unintended effects of SESTA/FOSTA on sex workers); Newton, *supra* note 34. Other critics argue that the law has chilled free speech online. *See, e.g.*, Lindsay

Attorney General William Barr and the Department of Justice held a workshop dedicated to brainstorming ideas for section 230 reform.[95] Just a few months later, President Trump issued an executive order threatening to strip Twitter of its section 230 protections when it labeled one of his tweets as misinformation.[96] Against this backdrop, it is reasonable to think that even if the EARN IT Act does not pass, something like it almost certainly will in the near future.

II.
SPOTLIGHT ON FACEBOOK

This Part uses Facebook to illustrate how large, well-resourced tech companies use a mix of software and human content moderators to detect and report CSAM on their platforms. Of course, because actively searching for CSAM is completely voluntary, tech platforms with different incentives and resources approach CSAM differently. For example, Facebook has fifteen thousand content moderators while Pornhub may have as low as eighty.[97] Facebook is a highly scrutinized, well-resourced company with 3.2 billion unique monthly users across its services (including WhatsApp and Instagram),[98] so it has both the incentives and means to keep its platform free from CSAM. Smaller, less mainstream companies are probably doing far less. Still, as this Section shows, even a large company like Facebook falls far short in its voluntary approach to CSAM. Thus, in its attempt to increase and standardize the way tech platforms approach CSAM, the EARN IT Act would dramatically affect all tech platforms, even large ones like Facebook.

As Facebook explained in a 2018 update, the company uses "photo-matching technology to stop people from sharing known child exploitation images," and is also experimenting with artificial intelligence that could detect previously unknown CSAM.[99] Facebook also has "specially trained teams with

---

Van Dyke, *How a Sex Trafficking Law Is Fundamentally Changing the Internet*, VICE NEWS (July 16, 2020), https://www.vice.com/en/article/4ay4eg/a-sex-trafficking-law-is-fundamentally-changing-the-internet [https://perma.cc/QAF7-RB74].

95. William P. Barr, Att'y Gen. of the U.S., Opening Remarks at the DOJ Workshop on Section 230: Nurturing Innovation or Fostering Unaccountability? (Feb. 19, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-opening-remarks-doj-workshop-section-230 [https://perma.cc/24RS-SWW2]. More recently, Justice Thomas called for a reimagining of tech regulations. *See* Biden v. Knight First Amendment Inst. at Columbia Univ., 141 S.Ct. 1220, 1221 (mem.) (2021) (Thomas, J., concurring) (suggesting that section 230 is outdated and that tech platforms might instead be regulable as "common carriers").

96. Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (June 2, 2020).

97. *See* Kristof, *supra* note 8. Of course, not all fifteen thousand of Facebook's content moderators work exclusively on CSAM. Content moderators filter out other objectionable material like disinformation or images of self-harm. *See* Zoe Thomas, *Facebook Content Moderators Paid to Work From Home*, BBC NEWS (Mar. 18, 2020), https://www.bbc.com/news/technology-51954968 [https://perma.cc/Z59F-2C2Z].

98. *See* Lawrence Nga, *Forget Tesla. Facebook Is A Better Buy Now*, MOTLEY FOOL (Dec. 29, 2020), https://www.fool.com/investing/2020/12/29/forget-tesla-facebook-is-a-better-buy-now/ [https://perma.cc/RWE8-6K3Y].

99. Davis, Facebook Press Release, *supra* note 85.

backgrounds in law enforcement, online safety, analytics, and forensic investigations" that review content manually and can report it directly to NCMEC.[100] At least some of those "specially trained teams" consist of content moderators: workers tasked with sifting through some of the most disturbing content on the internet in order to keep Facebook's service clean.[101] Broadly speaking, the company's approach boils down to two main tools: photo-matching supported by a software program called PhotoDNA and human moderation.

While most of Facebook's internal procedures are private, the following description comes from publicly available information as well as from original interviews with Dr. Farid, creator of PhotoDNA, and three current and former content moderators for Facebook.[102]

A. PhotoDNA

PhotoDNA is a photo-matching tool jointly created in 2009 by Microsoft and Dr. Farid, then a computer science professor at Dartmouth University and now at the University of California, Berkeley.[103] It was initially used internally at Microsoft, but the company subsequently donated the program to NCMEC, which now owns it and licenses it to tech platforms. Facebook implemented it in 2011.[104]

Importantly, Facebook only uses PhotoDNA to scan unencrypted photos.[105] Whenever a user uploads such a photo to Facebook (or its subsidiary, Instagram), that photo gets scanned by the PhotoDNA program.[106] But according to Dr. Farid, photos sent through apps like Signal or Facebook's WhatsApp, which both use end-to-end encryption to protect users' privacy, are far more difficult to scan

100. *Id.*

101. *See* Newton, *The Trauma Floor*, *supra* note 78; Newton, *Bodies in Seats*, *supra* note 78.

102. I interviewed the content moderators in late 2019. I interviewed Dr. Farid in late 2019 and again in April 2020. Because they had signed nondisclosure agreements, the content moderators requested to remain anonymous. Without naming them, I have nevertheless cited to their interviews throughout this Section.

103. Keller & Dance, *Child Abusers Run Rampant as Tech Companies Look the Other Way*, *supra* note 17.

104. Catharine Smith, *Facebook Adopts Microsoft PhotoDNA to Remove Child Pornography*, HUFF POST (May 20, 2011), https://www.huffpost.com/entry/facebook-photodna-microsoft-child-pornography_n_864695 [https://perma.cc/6582-4UP7].

105. Hany Farid, Opinion, *Facebook's Encryption Makes It Harder to Detect Child Abuse*, WIRED (Oct. 25, 2019), https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/ [https://perma.cc/7KHQ-D3TC]. Encryption is a complex process, but essentially it is a means by which two people can communicate without third parties being able to access the contents of the communication. With end-to-end encryption, only the sender and the receiver can view the material. For an excellent explanation of encryption, see Jeff Tyson, *How Encryption Works*, HOWSTUFFWORKS (Apr. 6, 2001), https://computer.howstuffworks.com/encryption.htm [https://perma.cc/Q8XX-8BGG].

106. While it is not a certainty that Facebook runs every single image through PhotoDNA, it is extremely likely that it does. According to Dr. Farid, scanning every image maximizes the effectiveness of PhotoDNA. He noted that Microsoft takes this approach with its cloud services. Dr. Farid Interview 1, *supra* note 16.

using PhotoDNA.[107] While recent advances in computer science suggest ways around this problem, there is no indication that Facebook scans end-to-end encrypted messages for CSAM, even as it expands access to encrypted services across its platforms.[108] As Dr. Farid puts it, this decision has created "a digital realm where images of child abuse can spread freely."[109]

PhotoDNA uses a hash algorithm to detect known CSAM imagery. Hash algorithms work by converting media like photographs into unique "hash codes," which are long strings of numbers.[110] Hash algorithms only work in one direction, meaning one cannot reverse engineer an image from a hash code.[111] Once PhotoDNA generates a hash code for a photo, it compares that code to the millions of hash codes in PhotoDNA's ever-growing database, each of which represents a known image of child sexual abuse or exploitation. If the program finds a match, it automatically flags the image, triggering Facebook's internal reporting procedures.[112] In addition to the image itself, Facebook may also include other information, such as the user's username or IP address, in its report to NCMEC.[113] Once Facebook detects and reports a CSAM image, it is bound by statute to preserve the image as evidence.[114]

Unlike traditional hash algorithms, which might generate wildly different hash codes for two images that are only one pixel apart from each other, PhotoDNA's algorithm accounts for similarities between images.[115] The program uses a process called fuzzy hashing, which means that similar photographs will generate similar hash codes.[116] The software can then quantify the differences between these hash codes to determine just how similar the photos are. Because of fuzzy hashing, PhotoDNA is sophisticated enough to detect when a seemingly new CSAM image is really just a modified version of a previously known one.[117] Therefore, a Facebook user cannot fool PhotoDNA

107. Interview with Dr. Hany Farid, Professor, U.C. Berkeley Sch. of Info., in Berkeley, Cal. (Apr. 20, 2020) [hereinafter Dr. Farid Interview 2]; Dr. Farid Interview 1, *supra* note 16.

108. *See* Dr. Farid Interview 2, *supra* note 107; Dr. Farid Interview 1, *supra* note 16.

109. Dr. Farid Interview 1, *supra* note 16.

110. *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna [https://perma.cc/X45F-3EZT].

111. *Id.*

112. Dr. Farid Interview 1, *supra* note 16; Interview with Anonymous Content Moderator No. 1, in Walnut Creek, Cal. (Oct. 26, 2019) [hereinafter Interview with CM1].

113. *See* 18 U.S.C. § 2258A (describing the information tech companies may choose to include in CyberTipline reports to NCMEC); *see also* United States v. Ackerman (*Ackerman I*), No. 13-10176, 2014 WL 2968164, at *3 (D. Kan. July 1, 2014) (explaining that when an image transmitted via AOL's email service is identified as CSAM, AOL transmits the entire email, the sender's IP address, and the sender's username to NCMEC), *rev'd on other grounds*, 831 F.3d 1292 (10th Cir. 2016).

114. 18 U.S.C. § 2258A(h).

115. Dr. Farid Interview 1, *supra* note 16.

116. *Id.*; Justin Paine & John Graham-Cumming, *Announcing the CSAM Scanning Tool, Free for All Cloudflare Customers*, CLOUDFLARE BLOG (Dec. 18, 2019), https://blog.cloudflare.com/the-csam-scanning-tool/ [https://perma.cc/47AM-GYJT] (explaining fuzzy hashing).

117. Dr. Farid Interview 1, *supra* note 16.

by simply converting an image to black and white, flipping it upside down, or extracting a still from a video of known CSAM.

Dr. Farid was reluctant to reveal the precise limits of PhotoDNA in our interview given its active use, but he explained that the program can be calibrated to detect higher or lower degrees of variation.[118] Allowing more variation increases the chances that PhotoDNA will detect CSAM that has been modified from its original form, but also increases the error rate. Conversely, allowing less variation leads to fewer errors but potentially misses some CSAM imagery. Dr. Farid explains that the baseline error rate for PhotoDNA is around one in fifty billion.[119] Even for a company like Facebook, with hundreds of millions of daily photo uploads, that translates to only a handful of errors each year—near 100 percent accuracy.[120]

Tech companies have been resistant to adopt PhotoDNA or similar software, and Dr. Farid says that some have procrastinated for years.[121] Pornhub, for example, only began voluntarily reporting to NCMEC in early 2020.[122] Cloudflare, which provides network infrastructure for millions of customers, began offering a PhotoDNA-like CSAM scanning tool in late 2019, a welcome but tardy move.[123] By now, PhotoDNA is over ten years old and in need of an update.[124] As hashing technology continues to advance, it will be up to tech companies to actually adopt it and apply it to finding CSAM.

B. Content Moderators

PhotoDNA's non-universal adoption and inability to scan encrypted images are two of its key weaknesses. A third is that it can only identify *previously known* CSAM imagery—imagery already in its database.[125] Barring any breakthrough technologies, new CSAM imagery must still be discovered, analyzed, and labelled by humans. That is where Facebook's content moderation teams come into play. They review material reported by Facebook's users and also review photos previously flagged by Facebook's algorithms as potential CSAM.[126] Considering the horrific yet critical nature of their work, it is worth

118. *Id.*

119. *Id.*; Dr. Farid Interview 2, *supra* note 107.

120. *See* Cooper Smith, *Facebook Users Are Uploading 350 Million New Photos Each Day*, BUS. INSIDER (Sept. 18, 2013), https://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9 [https://perma.cc/DQ5Z-CZWV].

121. Dr. Farid Interview 2, *supra* note 107.

122. Kristof, *supra* note 8.

123. Andrew Orr, *Apple Now Scans Uploaded Content for Child Abuse Imagery (Update)*, MAC OBSERVER (Oct. 25, 2019), https://www.macobserver.com/analysis/apple-scans-uploaded-content/ [https://perma.cc/EZ5V-KU79]; Paine & Graham-Cumming, *supra* note 116.

124. To underscore Facebook's low commitment to CSAM detection, Dr. Farid challenged me to name "one other technology at Facebook that is more than 10 years old." I could not. Dr. Farid Interview 1, *supra* note 16.

125. *Id.*

126. Interview with CM1, *supra* note 112; Interview with Anonymous Content Moderator No. 2., in Oakland, Cal. (Nov. 1, 2019) [hereinafter Interview with CM2].

pausing to examine a typical content moderator's employment conditions. Such an examination will also paint a more holistic picture of Facebook's unsatisfactory approach to the CSAM problem.

The vast majority of Facebook's content moderators are independent contractors working for firms like Accenture and Cognizant.[127] They are low-level workers making somewhere in the neighborhood of twenty dollars per hour and reviewing thousands of images per week.[128] They specialize in certain areas, like CSAM, hate speech, or violence.[129] The moderators I spoke to had seen some truly horrific things, including live murders and suicides, acts of terrorism, and animal abuse.[130] Not surprisingly, many content moderators suffer from post-traumatic stress disorder in much the same way human rights workers do.[131] The Accenture moderators I interviewed described having little mental health support and feeling like second-class citizens compared to Facebook's full-time employees.[132] Arguably, their poor working conditions and low pay demonstrate that even large companies like Facebook may not be taking the CSAM problem seriously enough. Indeed, this lack of effort, broadly speaking, is the very problem that the EARN IT Act attempts to solve.

When a content moderator reviews an image of suspected CSAM, they must make two determinations. The first is whether the image violates Facebook's terms of use. The second is whether the image should be reported to NCMEC.[133] Roughly speaking, their decisions are made according to the following tree:

---

127. *See* Newton, *The Trauma Floor*, *supra* note 78; Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126.

128. *See supra* note 78 (collecting articles describing the difficult working conditions of content moderators); Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Telephone Interview with Anonymous Content Moderator No. 3 (Jan. 4, 2020) [hereinafter Interview with CM3].

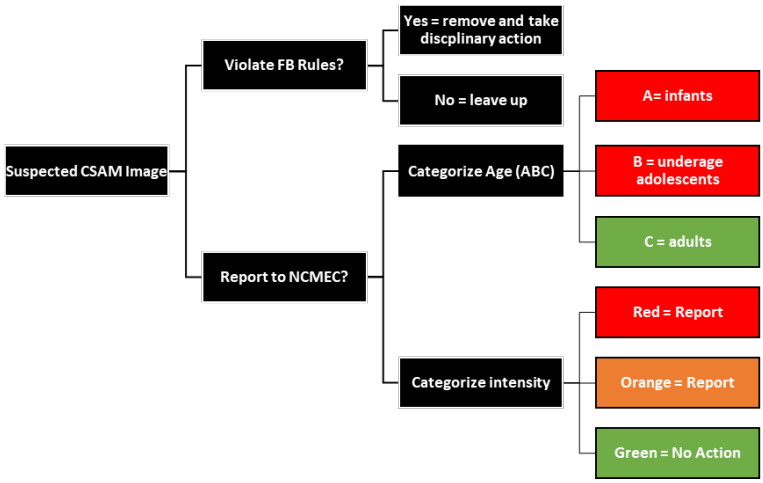
129. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

130. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

131. *See* Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128. Facebook recently settled a class action suit led by a former content moderator for $52 million. *See* Bobby Allyn, *In Settlement, Facebook to Pay $52 Million to Content Moderators with PTSD*, NPR (May 12, 2020), https://www.npr.org/2020/05/12/854998616/in-settlement-facebook-to-pay-52-million-to-content-moderators-with-ptsd [https://perma.cc/UK8X-KYWA]. For discussion of trauma in the closely related field of open source human rights investigations, see Elise Baker, Eric Stover, Rohini Haar, Andrea Lampros & Alexa Koenig, *Safer Viewing: A Study of Secondary Trauma Mitigation Techniques in Open Source Investigations*, 22 HEALTH & HUM. RTS. J. 293 (2020).

132. Interview with CM1, *supra* note 112; Interview with CM3, *supra* note 128.

133. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.



A decision tree I created from my own reporting. This is not an official Facebook document.

In determining whether to report an image to NCMEC, content moderators categorize both the age of the subject and the intensity of the activity in a suspected CSAM image.[134] For example, a video of a mother breastfeeding her child would be categorized as "A," containing imagery of an infant.[135] But the activity level would be "green," as in "not abusive."[136] This image may or may not violate Facebook's ever-shifting community guidelines, but because it does not depict child abuse it would not be reported to NCMEC.[137]

These categorizations are made under the guidance of internal policies at Facebook that incentivize inaction. Recently, for example, Facebook pushed out a new rule that images of girls with bare breasts will not be reported to NCMEC.[138] Nor will images of young children in sexually suggestive clothing. Interviewees also described a policy called "bumping up," which each of them personally disagreed with.[139] The policy applies when a content moderator is unable to readily determine whether the subject in a suspected CSAM photo is a minor ("B") or an adult ("C"). In such situations, content moderators are instructed to assume the subject is an adult, thereby allowing more images to go

134. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

135. *See* Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

136. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

137. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

138. Interview with CM3, *supra* note 128. This content moderator also worked as an auditor, a worker who double checks the decisions of other content moderators.

139. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

unreported to NCMEC.[140] The origins and rationales behind these policies are unclear, but they almost certainly result in underreporting to NCMEC. One rationale could be to prevent false positives from entering the PhotoDNA database, which could result in misguided and wasteful investigations. Another could be to make Facebook look good—the less CSAM it reports, the better it looks.

But how do content moderators reliably estimate a subject's age from a photo? After all, the images they view may be out of context, edited, or obscured. Content moderators at Facebook use something called the Tanner scale—a tool doctors and scientists use to categorize the different stages of puberty in adolescents.[141] The scale was designed in the mid-twentieth century after researchers, led by James Tanner, conducted a longitudinal study of a large cohort of children who lived in the England's National Children's Home, a place for children with disabilities, living in poverty, or suffering from neglect.[142] Tanner followed the children from infancy through adolescence, photographing them as they progressed through puberty.[143] With this data, Tanner was able to divide up the process of puberty into five stages.[144] When viewing suspected CSAM images, Facebook content moderators refer to a chart with illustrations of each of Tanner's five stages of puberty and attempt to categorize the subjects of the images according to their pubertal stage.

Since the scale was designed to measure the stages of puberty, not estimate age, the use of the Tanner scale is inappropriate for use in a child pornography setting. This is because CSAM has to do with a child's age, not pubertal stage. Two children of the same age but in different stages of puberty should not be treated unequally in the CSAM context, but relying on the Tanner scale means that more physically developed children are less likely to be identified as victims of sexual abuse. As Dr. Tanner himself wrote in a letter to the editor published in *Pediatrics* magazine in the late 1990s, "no equations exist estimating age from [Tanner] stage."[145]

---

140. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126; Interview with CM3, *supra* note 128.

141. *See, e.g.*, *Puberty: Is Your Daughter On Track, Ahead or Behind?*, CLEVELAND CLINIC: HEALTH ESSENTIALS (Dec. 28, 2017), https://health.clevelandclinic.org/puberty-in-girls-whats-normal-and-whats-not/ [https://perma.cc/P6E4-32L8]; Elly Den Hond & Greet Schoeters, *Endocrine Disruptors and Human Puberty*, 29 INT'L J. ANDROLOGY 264 (2006) (referring to stages of puberty in terms of the Tanner scale); Maria E. Bleil, Cathryn Booth-LaForce & Aprile D. Benner, *Race Disparities in Pubertal Timing: Implications for Cardiovascular Disease Risk among African American Women*, 36 POPULATION RSCH. POL'Y REV. 717 (2017) (same).

142. *See* Celia Roberts, *Tanner's Puberty Scale: Exploring the Historical Entanglements of Children, Scientific Photography and Sex*, 19 SEXUALITIES 328, 330–31 (2016).

143. *Id.* at 330–32.

144. *Id.* at 335.

145. Arlan L. Rosenbloom & James M. Tanner, *Misuse of Tanner Puberty Scale to Estimate Chronologic Age*, 102 PEDIATRICS 1494 (1998) (letter to the editor). I am not aware of any research suggesting that this statement is any less true today.

Even worse, the scale likely has a racial and gender bias. Because the subjects of the study were mostly white children, the Tanner scale does not account for differences in bodily development across race—nor does it attempt to.[146] Yet it is well known to pediatricians today that Black and Hispanic children tend to progress through the Tanner stages faster, perhaps reaching a visually "matur[e]" pubertal stage much earlier than they reach the legal age of consent.[147] Moreover, research suggests that girls tend to hit puberty earlier today than they did at the time the Tanner scale was developed.[148] Thus, *even if* the Tanner scale were perfect at estimating the age of white children at the time it was created (which, remember, it was not designed to do), it would still result in the underreporting of Black and female victims, all else being equal.

The content moderators I interviewed described this racial and gender bias as obvious, and related situations in which they were forced by Facebook's use of the Tanner scale to refrain from reporting images they strongly suspected were CSAM.[149] Indeed, the Tanner scale is so flawed that I suspect Facebook only uses it so that it can claim it has *some* system in place for its content moderators to use. In the best-case scenario, Facebook is actively working with other companies to develop more intelligent ways to confront new CSAM imagery. The worst case is that Facebook simply does not care to do more because, legally speaking, it does not have to. Either way, it is clear that more research is needed to improve the accuracy of age determinations in suspected CSAM imagery. The EARN IT Act would incentivize this additional research.

As a rule, all decisions by content moderators are double-checked by auditors, also low-level independent contractors, though in practice some auditors simply rubber stamp whatever action the first content moderator took.[150] From there, the report goes to NCMEC.

---

146. *See* Roberts, *supra* note 142, at 339.

147. *See, e.g.*, Bleil et al., *supra* note 141, at 718 (explaining that African American girls "experience more accelerated sexual maturation as assessed by several indicators of pubertal development" and collecting sources to support this claim); Samantha F. Butts & David B. Seifer, *Racial and Ethnic Differences in Reproductive Potential Across the Life Cycle*, 93 FERTILITY & STERILITY 681 (2010) (finding "earlier puberty in blacks and Hispanics compared with whites"), Marcia E. Herman-Giddens, Eric J. Slora, Richard C. Wasserman, Carlos J. Bourdony, Manju V. Bhapkar, Gary G. Koch & Cynthia M. Hasemeier, *Secondary Sexual Characteristics and Menses in Young Girls Seen in Office Practice: A Study from the Pediatric Research in Office Settings Network*, 99 PEDIATRICS 505, 508 (1997) (discussing racial differences in onset of various indices of puberty).

148. *See* Herman-Giddens et al., *supra* note 147, at 511 ("This study strongly suggests that earlier puberty is a real phenomenon . . . ."); Marcia E. Herman-Giddens, *Puberty is Starting Earlier in the 21st Century*, *in* WHEN PUBERTY IS PRECOCIOUS: SCIENTIFIC AND CLINICAL ASPECTS 105 (Ora H. Pescovitz & Emily C. Walvoord eds., 2007); Lise Aksglaede, Kaspar Sørensen, Jørgen H. Petersen, Niels E. Skakkebæk & Anders Juul, *Recent Decline in Age at Breast Development: The Copenhagen Puberty Study*, 123 PEDIATRICS 932 (2009) (finding that European girls, like American girls, are hitting puberty earlier).

149. Interview with CM1, *supra* note 112; Interview with CM2, *supra* note 126.

150. Interview with CM2, *supra* note 126 (former auditor); Interview with CM3, *supra* note 128 (current auditor).

C. NCMEC and Law Enforcement

Once a photo is reported to NCMEC, it is reviewed by NCMEC's analysts. NCMEC employs a three-way verification system, meaning that three analysts must independently determine that the material is CSAM before it is added to the PhotoDNA database.[151] NCMEC controls the database, and only NCMEC can decide whether an image should be added to it. If the photo is indeed CSAM, NCMEC takes additional steps to support law enforcement efforts. It might, for example, check the IP address of the user who posted or sent the CSAM, determine the user's location, or notify local police.[152]

III.
GOVERNMENT AGENCY TESTS AND CURRENT JURISPRUDENCE

In Part IV, I argue that the EARN IT Act implicates the Fourth Amendment by effectively coercing tech companies into acting as government agents with respect to the detection of CSAM and enforcement of CSAM laws. Here in Part III, I provide an overview of Supreme Court and circuit court jurisprudence about when private action might properly be considered government action for constitutional purposes. I also examine the most important recent case about CSAM, *United States v. Ackerman*, where the Tenth Circuit found that NCMEC is a government entity for Fourth Amendment purposes.[153] Next, this Section surveys the aftermath of *Ackerman* as well as courts' willingness to categorize tech companies as government agents thus far.

A. Government Entities and Government Agents

The Fourth Amendment protects citizens from unreasonable government searches and seizures.[154] While it generally "does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative," the Fourth Amendment does apply if "the private party acted as an instrument or agent of the Government."[155] A private actor, like a tech company, may be considered a government instrument in one of two ways. First, if it is closely tied to the government, a corporation that was not created by the government may nevertheless be considered a government entity—and thus "Government

151. Dr. Farid Interview 2, *supra* note 107.

152. *Id.*; *see also Ackerman I*, No. 13-10176, 2014 WL 2968164, at *3–4 (D. Kan. July 1, 2014) (describing how NCMEC contacted a local police department's Internet Crimes Against Children Taskforce and shared defendant's IP address and user name), *rev'd on other grounds*, 831 F.3d 1292 (10th Cir. 2016).

153. *Ackerman II*, 831 F.3d 1292, 1295 (10th Cir. 2016).

154. U.S. CONST. amend. IV; Ohio v. Robinette, 519 U.S. 33, 39 (1996) (noting that the "touchstone of the Fourth Amendment is reasonableness" (quoting United States v. Jimeno, 500 U.S. 248, 250 (1991)).

155. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989) (articulating the quoted language and first citing United States v. Jacobsen, 466 U.S. 109, 113–14 (1984); then citing Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971); and then citing Burdeau v. McDowell, 256 U.S. 465, 475 (1921)).

itself"—for constitutional purposes.[156] Second, a private actor might be acting as a government agent intentionally, unwittingly, or because of government coercion.[157] Incidentally, the two most relevant case examples of both types of private action on behalf of the government concern railroads. Below, this Section explains both cases—*Lebron v. National Railroad*, where the Court explored whether a railroad was acting as a government entity, and *Skinner v. Railway Lab Executives*, where the Court inquired into the agency relationship between the Government and railroads in the context of a drug-testing scheme. Then, this Section explains how circuit courts have fleshed out the government agency principles established in *Skinner.*

First, we turn to government entities. In *Lebron*, the Supreme Court considered whether Amtrak violated the First Amendment by banning political ads from a marquee billboard in New York City's Penn Station.[158] Of course, Amtrak was only subject to First Amendment restrictions if it was a government entity or otherwise acting as an agent of the government. [159] The Court found that the rail transportation company Amtrak was a government entity.[160]

The Court considered several factors in its analysis. At the outset, the Court noted that Amtrak was created by federal statute to benefit the public by saving the country's passenger train industry.[161] Aspects of Amtrak's operations, such as the average speed of its trains and parts of its pricing scheme, were also dictated by statute.[162] Moreover, Amtrak's board of directors consisted mainly of government-appointed officials and was therefore subject to government control.[163] "It surely cannot be," the Court reasoned, "that government, state or federal, is able to evade the most solemn obligations imposed in the Constitution

156. Lebron v. Nat'l R.R. Passenger Corp., 513 U.S. 374, 378 (1995) (articulating this rule and finding that Amtrak was a government entity for purposes of the First Amendment); *see also* Burton v. Wilmington Parking Auth., 365 U.S. 715 (1961) (holding a private parking garage operator excluding customers on the basis of race was state action because building was publicly financed and owned by state agency).

157. *See Skinner*, 489 U.S. at 615 (finding that railways act as government agents when they drug test employees pursuant to a government statute that strongly encourages such drug testing); United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003) (explaining the rule and collecting cases); United States v. Silva, 554 F.3d 13, 18–19 (1st Cir. 2009) (same).

158. *Lebron*, 513 U.S. at 376–78.

159. *Id.* at 377.

160. *Id.* at 394 (concluding that Amtrak is "an agency or instrumentality of the United States for the purpose of individual rights guaranteed against the Government by the Constitution"). The Tenth Circuit in *Ackerman II* analogized primarily to this case when it held that NCMEC was a government entity. *See Ackerman II*, 831 F.3d 1292, 1297–99 (10th Cir. 2016). The Supreme Court reaffirmed its holding in *Lebron* in *Department of Transportation v. Association of American Railroads*, 575 U.S. 43 (2015).

161. *Lebron*, 513 U.S. at 383–84. For a succinct history of government-created corporations, see *id.* at 386–91. For a more thorough version which incorporates the *Lebron* decision, see KEVIN R. KOSAR, CONG. RSCH. SERV., RL30365, FEDERAL GOVERNMENT CORPORATIONS: AN OVERVIEW (2011), https://fas.org/sgp/crs/misc/RL30365.pdf [https://perma.cc/7PPH-DWM6].

162. *Lebron*, 513 U.S. at 384–85.

163. *Id.* at 385–86.

by simply resorting to the corporate form."[164] After all, the Court contended, if the government could simply outsource its actions to corporations, Constitutional protections would be meaningless.[165] Therefore, the Court concluded, Amtrak was a government entity for purposes of the Fourth Amendment.[166]

If a corporation is found to be a government entity, then, for the purposes of the Constitution, the corporation is "Government itself."[167] But a corporation's actions may still be considered government action even if it is not a government entity.[168] In *Skinner v. Railway Labor Executives' Association*, the Supreme Court's leading case on the subject, the Court held that a private corporation could act as the government's agent in the context of the Fourth Amendment, even if the government regulation upon which the corporation acted was permissive and not mandatory.[169]

Skinner arose out of a challenge to regulations designed to address the prevalence of alcohol and drug use by railway employees.[170] Drug use was pervasive and had caused deadly accidents in the railway industry despite railway companies' broad prohibitions on the use of alcohol and drugs in the workplace.[171] In response, the Federal Railroad Administration (FRA) issued a two-pronged drug testing policy for railroads. The first prong was mandatory: it compelled railways to drug test employees after an accident.[172] The second prong was permissive: it authorized, but did not compel, railways to drug test employees at other times as well.[173] Still, the FRA laid out detailed protocols for railways to follow if they did choose to conduct these permissive drug tests.[174]

The threshold question in *Skinner* was whether railways acted as government agents when implementing the FRA's two-pronged drug testing policy.[175] The Court held that the mandatory, post-accident drug tests were government action because companies were compelled to conduct them.[176] But, importantly for our purposes, the Court also held that the permissive drug tests

164. *Id.* at 397.

165. *See id.* (pointing out that states could "resurrect[]" *Plessy v. Ferguson* by using Amtrak to operate segregated trains).

166. *Id.* at 394.

167. *Id.* at 397.

168. *Id.* at 378 ("[A]ctions of private entities can sometimes be regarded as governmental action for constitutional purposes."); Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989) (explaining that the Fourth Amendment protects against searches by a private party "if the private party acted as an instrument or agent of the Government" and first citing United States v. Jacobsen, 466 U.S. 109, 113–14 (1984); then citing Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971); and then citing Burdeau v. McDowell, 256 U.S. 465, 475 (1921)).

169. *Skinner*, 489 U.S. at 615.

170. *Id.* at 606–07.

171. *Id.* at 606–09.

172. *Id.* at 609–11.

173. *Id.* at 611–12.

174. *Id.*

175. *Id.* at 613–14.

176. *Id.* at 614.

constituted government action.[177] The Court established at the outset that "whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes" depends on the degree of government participation and is therefore a question that can only be resolved "in light of all the circumstances."[178]

The Court's discussion of the permissive tests centered on the inducements created by the statute that strongly encouraged Amtrak to implement regular drug testing of its employees. The Court pointed to the fact that Congress had barred railroads from contracting away their statutory authority to conduct drug tests as evidence of the government's strong encouragement and endorsement.[179] Furthermore, employees were not free to refuse the testing.[180]

While nothing in the regulation would have punished the railway companies for simply refusing to drug test, the Court noted that the government had "removed all legal barriers" to the permissive testing and in doing so had "made plain not only its strong preference for testing, but also its desire to share in the fruits of such intrusions," ostensibly by reducing fatalities and increasing the overall efficiency of the nation's railways.[181] The Court found that these features of the regulation were "clear indices of the Government's encouragement, endorsement, and participation, and suffice[d] to implicate the Fourth Amendment."[182] In short, the government "did more than adopt a passive position toward the underlying private conduct."[183] Therefore, despite the voluntary nature of the regulation, the Court found an agency relationship between the railways and the government because the government wanted drug testing, benefitted from it, and made it easier for railways to test for drugs.[184]

While *Skinner* did not formally articulate a definitive government agent test, many circuit courts have. Their approaches range from multi-factor tests to simple reliance on "common law principles," but they rely on many of the same considerations that *Skinner* and *Lebron* did. What follows is a survey of different circuit tests. The reader will notice that they converge around three major factors: 1) government encouragement or participation; 2) government benefits; and 3) the private actor's independent motivations.

The First and Ninth Circuits use multi-factor tests when examining whether a private actor has behaved as a government agent. Courts in the First Circuit look to 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 aims

177. *Id.* at 614–15.
178. *Id.* at 614–15 (citing Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).
179. *Id.* at 615.
180. *Id.*
181. *Id.*
182. *Id.* at 615–16.
183. *Id.* at 615.
184. *See id.*

primarily to help the government or to serve its own interests."[185] The Ninth Circuit distills these considerations into two "critical" factors: 1) "the government's knowledge and acquiescence," and 2) "the intent of the party performing the search."[186] With respect to the first factor, the Ninth Circuit has cautioned that "[m]ere governmental authorization [of the search] in the absence of more active participation or encouragement" is not enough to implicate the Fourth Amendment.[187] Rather, the level of government involvement is to be assessed on a case-by-case basis.[188]

The Fourth and Seventh Circuits' approaches are less precise. The Fourth Circuit has held that the government agent question should be "guided by common law agency principles."[189] The Fourth Circuit also looks to the Seventh Circuit's analysis, which simply asks "whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further her own ends."[190] As the Tenth Circuit notes, however, the mere existence of independent reasons for the challenged conduct does not end the inquiry.[191] Instead, the question in common law is "usually simply whether the agent acts with the principal's consent and (in some way) to further the principal's purpose."[192] In general, when conducting a Fourth Amendment government agent analysis, courts require some level of government knowledge, encouragement, or acquiescence. Some courts, however, also consider whether the alleged agent had independent reasons for acting.[193] While not usually dispositive, this may press against a finding that the private actor was a government agent. Notably, even though the railway companies in *Skinner* presumably had independent reasons for drug testing their employees (like safety and protecting assets), the Supreme Court did not discuss those motivations in its Fourth Amendment government agency inquiry.[194]

---

185. United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009).

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

187. *Id.*

188. *Id.* at 791 (explaining that "there exists a gray area between the extremes of overt governmental participation in a search and [the] complete absence of such participation" (internal quotations omitted)).

189. United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003). The Fourth Circuit requires that the government "do more than passively accept or acquiesce in a private party's search efforts." United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003).

190. *Ellyson*, 326 F.3d at 527 (quoting United States v. Feffer, 831 F.2d 734, 739 (7th Cir.1987)).

191. *Ackerman II*, 831 F.3d 1292, 1301 (10th Cir. 2016) ("Neither has the common law traditionally required that the agent be an altruist, acting without any intent of advancing some personal interest along the way (like monetary gain). As clients know well, lawyers can serve as their agents all while zealously charging by the hour.").

192. *Id.*

193. *See* United States v. Feffer, 831 F.2d 734, 739 (7th Cir.1987); United States v. Gomez, 614 F.2d 643, 645 (9th Cir. 1979) ("A carrier's search, on its own initiative, for its own purposes, is normally considered a private (and not a governmental) search, and thus not one giving rise to Fourth Amendment protections.").

194. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 606–16 (1989).

B. United States v. Ackerman and Tech Companies as Government Agents Today

The Supreme Court has not applied the government entity or agency tests in the CSAM context, but lower courts have done so increasingly often. The most important such case is *United States v. Ackerman (Ackerman II)*.[195] Notably, it was authored by Supreme Court Justice Neil Gorsuch during his time as a Tenth Circuit federal judge. The Tenth Circuit held that NCMEC, the private nonprofit clearinghouse for CSAM, is a government entity. *Ackerman II* concerned a criminal defendant's motion to suppress evidence used in his prosecution for violations of CSAM laws.[196] Using his AOL account, Ackerman sent an email message with four images attached. AOL's internal photo-matching algorithm, similar to PhotoDNA, scanned all four attachments and identified one as containing previously known CSAM.[197] AOL flagged the email and automatically generated a report to NCMEC. It forwarded the entire email file, including all four attachments, as part of the report.[198] An NCMEC analyst opened all four attachments, not just the one flagged by AOL, and found that all four contained CSAM.[199] NCMEC then notified local law enforcement officials, who arrested Ackerman.[200] Shortly thereafter, Ackerman was indicted on child pornography charges.[201]

Ackerman alleged that both AOL and NCMEC acted as agents of the government—AOL when it searched Ackerman's email communication for CSAM and forwarded it to NCMEC and NCMEC when it searched Ackerman's email for additional CSAM and tipped off law enforcement.[202] In Ackerman's view, the photographs should have been suppressed as the result of an unreasonable search and seizure.[203]

On the appeal, the court considered two major questions: 1) Is NCMEC a governmental entity or agent for Fourth Amendment purposes? 2) If so, did NCMEC conduct a Fourth Amendment "search"? To both questions, the court answered yes.[204]

In considering the governmental entity question, the *Ackerman II* court relied heavily on *Lebron*, discussed at length in Part III.A, to conclude that

---

195. *Ackerman II*, 831 F.3d 1292 (10th Cir. 2016).

196. *Ackerman I*, No. 13-10176, 2014 WL 2968164, at *11 (D. Kan. July 1, 2014), *rev'd on other grounds*, 831 F.3d. 1292 (10th Cir. 2016).

197. *See Ackerman II*, 831 F.3d at 1294–95.

198. *Id.* at 1294.

199. *Id.*

200. *Id.*

201. *Id.*

202. *Ackerman I*, 2014 WL 2968164, at *4–6.

203. *Id.*

204. *Ackerman II*, 831 F.3d at 1295. The district court had dismissed Ackerman's contention that AOL was also a government entity because AOL was merely complying with a reporting requirement, not acting at the government's behest; this question was not put before the appeals court. *See infra* note 237.

NCMEC is indeed a governmental entity. The court noted that NCMEC, like Amtrak in *Lebron*, is authorized and governed by statute.[205] NCMEC is required to carry out "over a dozen separate functions, a fact that evinces the sort of 'day-to-day' statutory control over its operations that the Court found telling present in [*Lebron*]."[206] As with Amtrak, the federal government participates in NCMEC's "daily operations."[207] Indeed, the federal government accounts for a majority of NCMEC's annual budget, and NCMEC's work on protecting children confers an enormous public benefit.[208] The court doubted NCMEC could escape classification as a governmental entity when Amtrak could not, given the "many unique law enforcement powers" that NCMEC was afforded.[209]

The court went on to reason that even if NCMEC did not qualify as a government entity, it still qualified as a government agent.[210] For this proposition, the court relied on *Skinner*, common law agency principles, and the several lower court government agency tests discussed in Part III.A.[211] Though the statutory scheme governing NCMEC did not explicitly require that it review emails like Ackerman's, the government authorized and funded the NCMEC's action and greatly benefited from the searches for CSAM law violations.[212] Indeed, Congress had "except[ed] [NCMEC] from the myriad laws banning the knowing receipt, possession, and viewing of child pornography."[213] The government's encouragement and endorsement of NCMEC's operations, combined with their clear law enforcement benefits, was enough for a finding of an agency relationship.[214] This echoes the reasoning in *Skinner*, where the statutory drug testing scheme was permissive, but Congress had "removed all legal barriers" to the railway companies carrying out drug tests.[215] In both cases, Congress signaled to private actors precisely what it wanted them to do and then made it easy to do precisely those things.

Additionally, as *Skinner* implied and as *Ackerman II* made explicit, the mere existence of independent reasons for the private action (like employee safety or monetary gain) does not defeat a finding of government action.[216] The

205. *Ackerman II*, 831 F.3d at 1297–98.
206. *Id.* at 1298.
207. *Id.*
208. *See id.* at 1297–98; *id.* at 1298 n.4 (citing to United States v. Keith, 980 F. Supp. 2d 33, 41 (D. Mass. 2013), and to publicly available information from the Department of Justice's Office of Juvenile Justice & Delinquency Prevention).
209. *Ackerman II*, 831 F.3d at 1298.
210. *See id.* at 1300–04.
211. *Id.*; *see* discussion *infra* Part III.A.
212. *Ackerman II*, 831 F.3d at 1302.
213. *Id.*
214. *See id.*
215. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989).
216. *See id.*; *Ackerman II*, 831 F.3d at 1301 ("Neither has the common law traditionally required that the agent be an altruist, acting without any intent of advancing some personal interest along the way (like monetary gain). As clients know well, lawyers can serve as their agents all while zealously charging by the hour.").

.

Ackerman II court pointed out that "agents routinely intend to serve their principals with the further intention to make money for themselves."[217] Thus, NCMEC's independent motivations for investigating CSAM did not on their own defeat the contention that it was a government agent.[218]

The second question was whether the actions of NCMEC, a government entity or agent, constituted a Fourth Amendment "search." The court relied on the "private search" doctrine to determine that NCMEC's actions did indeed constitute such a search.[219] Under the private search doctrine, the government conducts a Fourth Amendment search only if it expands the scope of a private party's search. On the other hand, if it merely replicates a search inspection conducted by a private party without expanding its scope, it has not conducted a Fourth Amendment search.[220] In *Ackerman II*, since NCMEC—a governmental entity—viewed all four attachments to Ackerman's email, as well as the email itself, it expanded the scope of AOL's private search, which flagged just one of the images as CSAM.[221]

The court also included a discussion, but no holding, about whether the examination of Ackerman's emails was a search for other reasons besides the private search doctrine. The court pointed out that emails, like letters, contain exactly the type of private, intimate information that the Fourth Amendment was drafted to protect.[222] Thus, a government entity arguably conducts a Fourth Amendment search when it reads someone's email without a warrant. Yet, the court noted, Ackerman's expectation of privacy in those emails might be diminished by the so-called third-party doctrine, which states that people have a diminished privacy interest in information—like bank deposit slips—they voluntarily turn over to third parties.[223] Since Ackerman had enlisted a private carrier to transmit his message, perhaps he, too, had a diminished privacy interest in his emails. However, because the third-party doctrine's applicability to private email messages has yet to be conclusively determined by the courts, and because the lower court had not considered it, the Tenth Circuit relied on the private search doctrine instead.[224]

Even still, it is important to remember that *Ackerman II* was a bombshell decision. Courts around the country have begun to accept *Ackerman II's* conclusion that NCMEC is a governmental entity or agent, increasingly leaving

217. *Ackerman II*, 831 F.3d at 1303.

218. *See id.*

219. *See id.* at 1305–07. As I discuss in more depth in Part V, if a government entity or agent's actions constitute a "search," the government must (in general) obtain a warrant.

220. *Id.* at 1305 (citing United States v. Jacobsen, 466 U.S. 109 (1984) for the rule).

221. *Id.* at 1306–07.

222. *See id.* at 1304.

223. *Id.* at 1304–05. The third-party doctrine is exemplified by *United States v. Miller*, 425 U.S. 435 (1976) (bank deposit slips) and *Smith v. Maryland*, 442 U.S. 735 (1979) (pen register recording dialed telephone numbers). The third-party doctrine is not absolute, and many legal scholars and court decisions indicate that it may soon undergo a radical change. I discuss this in detail in Part V.A(a).

224. *Ackerman II*, 831 F.3d at 1305. I discuss the third-party doctrine further in Part V.

tech companies as the only private actors in the equation.[225] Consider *United States v. Powell*, a post-*Ackerman II* case from the First Circuit concerning Omegle a video and text chat platform which turned over suspected CSAM to NCMEC. [226] In *Powell*, the court began its Fourth Amendment analysis with the assumption that "for all relevant purposes" NCMEC was acting as a government agent when it viewed the CSAM material Omegle reported, apparently adopting the Tenth Circuit's logic in *Ackerman*.[227] The court then focused on whether NCMEC's viewing of the imagery without a warrant violated the Fourth Amendment.[228] The court concluded that it did not because of the private search doctrine, which allows the government or its agents to simply replicate a search already conducted by a private party.[229] That private party, of course, was Omegle. Since Omegle viewed the material before turning it over to NCMEC, NCMEC could not have learned any "fact previously unknown" by viewing the material.[230] Therefore, NCMEC had not acted unconstitutionally. [231]

The results in *Ackerman II* and in *Powell* leave tech companies in the uncomfortable position of influencing whether NCMEC's actions are unconstitutional. Both cases relied on the private search doctrine to decide whether NCMEC, a governmental entity, expanded the original, private search conducted by a tech company. In *Powell*, NCMEC merely replicated Omegle's private search, but in *Ackerman II*, NCMEC expanded upon AOL's more limited search. In both cases, the tech companies' original actions were central to the constitutional inquiry, a tricky position for a private actor.[232] If the EARN IT Act passes and converts the tech companies *themselves* into government agents,[233] the private search doctrine would be inapplicable: there would be no private actors left in the equation. Instead of subjecting only NCMEC's searches to constitutional scrutiny, courts would look directly at the searches carried out by tech companies themselves. Tech company searches for CSAM *would be* government searches for CSAM.

In a pre-EARN IT Act world, tech companies do not have much to worry about. Courts both before and after *Ackerman II* have almost universally rejected the argument that the companies *themselves* act as government agents when they

225. *See, e.g.*, United States v. Coyne, 387 F. Supp. 3d 387, 397–400 (D. Vt. 2018) (disagreeing with *Ackerman* that NCMEC is a governmental entity but concluding that NCMEC is a government agent for Fourth Amendment purposes).

226. United States v. Powell, 925 F.3d 1 (1st Cir. 2018).

227. *Id.* at 5.

228. *Id.*

229. *Id.* at 6.

230. *Id.* (quoting United States v. Jacobsen, 466 U.S. 109,122 (1984)).

231. *Id.*

232. This is likely one of the reasons Facebook, Dropbox, Google, and Snap, Inc. filed a joint amicus brief in *Ackerman II* encouraging the court to rule against Ackerman. Brief of Dropbox, Inc., Facebook, Inc., Google, Inc., Microsoft Corp., Pinterest, Inc., Snapchat, Inc., and Twitter, Inc. as Amici Curiae Supporting Appellee at 10–11, *Ackerman II*, 831 F.3d 1292 (10th Cir. 2016) (No. 14-3265), 2015 WL 4747925, at *6.

233. *See infra* Part IV.

search for and report instances of child pornography. The Fourth Circuit's reasoning in *United States v. Richardson*—another AOL case—is particularly sharp. There, the court distinguished *Skinner* because the enabling statute in *Skinner* encouraged railways to actively conduct drug tests and even laid out protocols for how to do so.[234] By contrast, far from encouraging tech companies to actively search for CSAM, federal law only requires them to report known instances of CSAM.[235] As the *Richardson* court pointed out, this scheme might actually encourage tech companies to "take steps to avoid discovering reportable information."[236]

Similarly, in *Ackerman I*, the district court swiftly rejected the notion that AOL was a government agent, reasoning that "[c]ompliance with a reporting statute . . . does not transform an internet service provider's private actions into government actions."[237] And in *United States v. Stratton*, the court found that Sony did not act as a government agent when it scanned its PlayStation Network for CSAM.[238] Like in *Richardson*, that Sony was not subject to a statutory scheme aside from its legal obligation to report known CSAM was critical to the court's analysis.[239] The *Stratton* court found it particularly important that the government did not ask Sony "to act affirmatively to monitor its users' accounts, review its users' downloads, or maintain any sort of reporting system for abuse" of Sony's systems."[240] The EARN IT Act, of course, would seek affirmative action.

In contrast to *Richardson*, *Stratton*, and *Ackerman I*, other courts have asked whether the tech company in question has independent reasons to scan for CSAM. In *United States v. Cameron*, the First Circuit reasoned that Yahoo! must have had independent reasons for scanning its users' emails for CSAM without even bothering to explore what those reasons might be.[241] The court in *United States v. Keith* also concluded that AOL did not qualify as a government agent even though it monitored user emails because the government "exercise[d] no control over AOL's monitoring of its network" and AOL had a "business interest" in monitoring its servers for criminal activity.[242]

Still, courts have not ruled out the possibility that tech companies can act as government agents. In *United States v. DiTomasso*, the District Court for the Southern District of New York assumed that two companies, AOL and Omegle, *could* act as government agents even if they had independent reasons for

234. United States v. Richardson, 607 F.3d 357, 366 (4th Cir. 2010).
235. *See supra* Part I.A; *Richardson*, 607 F.3d at 367.
236. *Richardson*, 607 F.3d at 367. Indeed, it is precisely this misalignment of incentives that the EARN IT Act seeks to address.
237. *Ackerman I*, No. 13-10176, 2014 WL 2968164, at *6 (D. Kan. July 1, 2014), *rev'd on other grounds*, 831 F.3d. 1292 (10th Cir. 2016).
238. United States v. Stratton, 229 F. Supp. 3d 1230, 1237–38 (D. Kan. 2017).
239. *Id.* at 1237.
240. *Id.*
241. *See* United States v. Cameron, 699 F.3d 621, 637 (1st Cir. 2012).
242. United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013).

scanning the defendant's emails and chats for child pornography.[243] There, the focus was on whether the defendant had nevertheless consented to the search by agreeing to the companies' terms of service.[244]

The *DiTomasso* court concluded that the defendant had consented to AOL's search of his emails by agreeing to AOL's terms of service.[245] The court noted AOL's terms of service explicitly stated that it did not tolerate illegal content and that AOL would actively assist law enforcement in response to illegal activity.[246] On the other hand, Omegle's terms of service were too vague and did not state its desire to work as an agent of law enforcement.[247] Thus, in agreeing to Omegle's terms of service, the defendant did not consent to Omegle's search of his chats as a government agent and could proceed with his constitutional claim.[248] This decision demonstrates that, even today, in a pre-EARN IT Act world, tech companies cannot count on being excluded from a Fourth Amendment analysis, and that analysis might even turn on the specific contents of their terms of service.

Because courts have generally avoided categorizing tech companies who report CSAM as government agents, these companies have been able to avoid difficult Fourth Amendment scrutiny. In the next Section, I demonstrate why legislation like the EARN IT Act would change the status quo and convert tech companies into government agents. Consequently, their current searches and scans of user data, as well as any future searches encouraged by the Commission, would be directly reviewable under the Fourth Amendment as government action.

IV.
THE EARN IT ACT AND DEPUTIZING TECH COMPANIES AS GOVERNMENT AGENTS

This Section argues that courts should consider tech companies government agents under the Act. In the Section below, I first refresh the reader's memory about the EARN IT Act. Then I analyze the EARN IT Act in light of the government entity or agency analyses explained in *Lebron* and *Skinner* and elaborated upon by the various circuit court cases discussed in Part III. In context, these principles are: 1) the government's level of encouragement and endorsement of tech companies following the Commission's guidelines in searching for and reporting CSAM; 2) the ways the government benefits from the EARN IT Act; and 3) tech companies' independent motivations for searching for CSAM. I conclude that while tech companies are not likely to be considered government entities under the Act, they are likely to be considered government

243. *See* United States v. DiTomasso, 56 F. Supp. 3d 584, 591–98 (S.D.N.Y. 2014).
244. *Id.* at 596–97.
245. *Id.*
246. *See id.* at 597–98.
247. *Id.* at 596–97.
248. *Id.*

agents, which will raise a new slate of Fourth Amendment questions for the courts. For example, courts would have to answer whether a PhotoDNA scan would be permissible under the Fourth Amendment and think through whether users of large tech platforms consented to government searches of their profiles. These issues are discussed in Part V.

A. The Status Quo and the EARN It Act: A Refresher

Recall from Part II that tech platforms are subject to only one statutory obligation regarding CSAM: they must report it to NCMEC only if they gain actual knowledge of it. This disincentivizes companies from proactively looking for CSAM.[249] Still, because of social or ethical incentives, large companies like Facebook go beyond the legal requirement and rely on a mixture of computer algorithms and human content moderators to root out CSAM. Some might deem these efforts inadequate. For instance, Facebook uses questionable triaging practices, does not currently scan its end-to-end encrypted services with PhotoDNA, and has not invested heavily in the well-being of its content moderation teams.

As Part I explained, the EARN IT Act would change the statutory landscape.[250] It would create a Commission populated by congressionally appointed experts, members of government, and industry representatives.[251] The Commission's job would be to develop recommended best practices for tech companies to implement when scanning for and reporting CSAM online.[252] While complying with these best practices is technically voluntary, companies that choose not to comply could face dire consequences.[253] The Act strips tech platforms of invaluable section 230 protections, exposing them to a potential flood of criminal and civil litigation over their role in spreading CSAM.[254] Compliance with the Commission's recommendations could provide a desperately needed shield against civil lawsuits and criminal enforcement actions.

In this Section, I argue that the current lack of effort from tech companies, the broad scope of the Commission's authority under the EARN IT Act, and the Act's section 230 carve-out add up to a law that deputizes tech companies as government agents in the enforcement of CSAM laws. To illustrate how, I compare the EARN IT Act to the statute at issue in *Skinner* and conclude that the Act would convert tech companies into government agents under principles established by *Skinner* and developed by lower courts.

---

249. *See supra* Part II.A–B and accompanying notes; *supra* Part I.A.
250. *See* discussion *supra* Part I.B.
251. *See supra* Part I.B.1 and accompanying notes.
252. *See supra* Part I.B.1 and accompanying notes.
253. *See supra* Part I.B.2 and accompanying notes.
254. *See supra* Part I.B.2 and accompanying notes.

B. Government Agency Analysis

Before diving into the government agency analysis, let us first dispense with the government *entity* analysis. As demonstrated by *Lebron*, in order for a company to qualify as a government entity, the government must exert a large amount of direct control over the entity in question.[255] This might include providing financing, making business decisions, and giving the entity statutory authority.[256] Similar factors were relevant for NCMEC in *Ackerman*.[257] Unlike Amtrak and NCMEC, tech platforms are not created by statute, do not enjoy many special government privileges (though section 230 arguably is one), and certainly do not allow the government to populate their boards. Thus, courts are not likely to consider tech companies government entities under the EARN IT Act or similar legislation.

It is more likely, however, for courts to consider tech companies government *agents* under the Act. In Part III.A, I explained the government agency tests. Remember, the basic rule from *Skinner* is that a private entity acts as a government agent when there are "clear indices of the Government's encouragement, endorsement, and participation" in a private company's actions.[258] The government must also "[do] more than adopt a passive position toward the underlying private conduct."[259] Thus, in *Skinner*, the railway was a government agency because, even though its drug testing regime was permissive, Congress had strongly expressed its desire for drug testing and had "removed all legal barriers" to action.[260] In applying *Skinner*, the circuit courts have considered factors such as the government's knowledge of, active participation in, encouragement of, or acquiescence to the challenged action.[261] Some courts have also factored in the independent motivations of the private actor, but remember that mere existence of independent incentives usually does not tilt the scales against agency.[262] In the next three sub-sections, I apply these factors to tech companies under an EARN IT Act regime.

1. Encouragement, Endorsement, and Participation

The EARN IT Act reflects the government's encouragement, endorsement, participation, and even coercion—important factors in the government agency analysis. If the scheme in *Skinner* was a nudge, the EARN IT Act is more like a shove.

---

255. *See* Lebron v. Nat'l R.R. Passenger Corp., 513 U.S. 374, 384–86 (1995).
256. *See id.*
257. *See supra* notes 205–209.
258. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615–16 (1989).
259. *See id.* at 615.
260. *Id.*
261. *See id.* at 602; *see supra* notes 185–193 and accompanying text (reviewing circuit court government agency tests).
262. *See supra* notes 185–193.

The EARN IT Act has coercive elements that were absent in the regulations at issue in *Skinner*, which makes it an even stronger example of government encouragement, endorsement, and participation. After creating the Commission, the Act promptly eviscerates section 230 protections—the "governing foundation of the internet"[263]—by exposing tech companies to potentially crushing litigation under federal and state law.[264] In essence, the government offers tech platforms a heavily skewed choice: they may either "choose" to follow the Commission's recommendations or expose themselves to an existential legal threat. Complying with recommendations that have the weight of the Justice Department behind them, especially with a potential flood of litigation on the line, seems less like a choice and more like the only option.[265] By complying with the recommendations and taking an active approach to finding CSAM, tech companies could avoid most litigation altogether. In the end, all roads lead to compliance.

Of course, even if compliance were truly voluntary, like the drug-testing scheme in *Skinner*, the government's encouragement and active participation would still lead to an agency relationship. As *Skinner* demonstrates, a private party need not face an existential threat in order to be considered a government agent. It is enough that the government express a strong desire for action—which the EARN IT Act does via the Commission's recommendations—and enable private actors to carry out the government's wishes smoothly.[266] In *Skinner*, in addition to authorizing the railways to drug test their employees, the government made it easier for railways to test by preempting state laws.[267] Similarly, the EARN IT Act creates legal protections that enable tech companies to help the government. For example, the Act allows tech companies to retain CSAM indefinitely in order to develop better technology and streamline law enforcement priorities—activity that would otherwise blatantly violate CSAM laws. This echoes the scheme in *Ackerman II* that "except[ed] [NCMEC] from the myriad laws banning the knowing receipt, possession, and viewing of child pornography."[268] Such activity is given special treatment "precisely because of the unique value it provides in the prosecution of child exploitation crimes"—a government function.[269] When considered in light of the section 230 carve-out described above, this legal protection seems more like a strong suggestion.

Additionally, the statutory scheme here is more comprehensive than the one in *Skinner*. The government in *Skinner* demonstrated its endorsement and

263. Romano, *supra* note 30.

264. *See supra* Part I.B(b).

265. As my high school teacher might say, this is not volunteering, it's volun*telling*. While companies could attempt to develop alternatives to the Commission's recommendations, it would likely be a waste of resources to invest heavily in alternatives that might never earn the government's blessing and may not hold up in court.

266. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 603, 615 (1989).

267. *See id.*

268. *Ackerman II*, 831 F.3d 1292, 1302 (10th Cir. 2016).

269. *See* S. 3398, 116th Cong. § 8 (2020); *Ackerman II*, 831 F.3d at 1297.

encouragement by laying out specific statutory protocols for the railways to follow in conducting drug tests.[270] The EARN IT Act goes even further: it creates a live Commission to complement existing laws and amendments enacted via the Act. The Commission would be primarily staffed by Congress and chaired by the chief law enforcement officer of the United States, the Attorney General.[271] It would likely tell tech companies exactly how to carry out the government's law enforcement priorities, including government-approved content moderator training programs and warrantless examinations of user profiles, messages, and data.[272]

Though the companies technically have a seat at the table, they may not end up with much of a say in the decisions made by the Commission. The Commission will only require fourteen out of nineteen members to agree to a proposed "best practice" before it is formalized.[273] Thus, as one commentator points out, the Commission could adopt a recommendation over the unanimous objection of the four industry representatives on the panel.[274] While this is less government control than the government-appointed board that controlled day-to-day Amtrak operations in *Lebron*, the Commission may in effect become a government-controlled board dictating CSAM related best practices for any company operating online.[275]

The EARN IT Act, like the scheme in *Skinner*, does "more than adopt a passive position toward the underlying private conduct."[276] The government wants private companies to assist in its law enforcement efforts, and it is willing to provide strong incentives for them to do so.

2. How the Government Benefits

In *Skinner*, the Court emphasized that the government not only encouraged the drug tests, but also benefitted from their being carried out.[277] Both the purpose and structure of the EARN IT Act demonstrate how the government will benefit from tech companies' actions if the Act becomes law.

Just as the government in *Skinner* was interested in promoting the efficiency of the railway system and the safety of railway employees, the government here is interested in promoting both the safety of children and

---

270. *See Skinner*, 489 U.S. at 611–12 (explaining how the statute lays out when railroads are authorized to drug test their employees and what protocols to follow in conducting the tests).

271. S. 3398 § 3(c)(1).

272. *See supra* Part I.B(a) and note 71.

273. S. 3398 § 4(a)(2).

274. Riana Pfefferkorn, *The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning It*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y: BLOG (Jan. 30, 2020), http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it [https://perma.cc/97X5-DFVU].

275. *See supra* notes 161–165 and accompanying text.

276. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989).

277. *See id.* at 603 (noting that that the statute "ma[de] plain a strong preference for testing and a governmental desire to share the fruits of such intrusions").

internet users and the effective enforcement of CSAM laws.[278] If the government tried to scan millions of private user accounts for CSAM, however, it could run into serious Fourth Amendment issues.[279] To date, private companies can do so without raising such concerns.[280] Thus, the EARN IT Act would ask tech companies to do what the government cannot by forcing them to search for CSAM while conforming nearly every aspect of their CSAM detection, prevention, research, and reporting protocols to government guidelines. The Act is therefore an overt example of the government seeking to "evade the most solemn obligations imposed in the Constitution by simply resorting to the corporate form."[281] Outsourcing its law enforcement duties to private companies while avoiding constitutional scrutiny is a clear benefit to the government.

But perhaps the clearest evidence of the government's interest in whether and how tech companies search for and report CSAM is the fact that the U.S. Attorney General will oversee the Commission responsible for creating guidelines for every internet-based company that could be touched by CSAM.[282] The government knows that it cannot prosecute online child sex abuse crimes without the help of tech companies. As the creation of the Commission alongside the section 230 carve-out suggests, the more active and uniform tech companies are in their approach to CSAM, including in the training of content moderators and implementation of photo-matching software, the easier it is for the government to achieve its law enforcement and public safety objectives.

Because of the unique role private tech companies play in assisting the government with enforcing of CSAM laws, it is difficult to deny that the government would, and wants to, benefit from tech companies' actions under the EARN IT Act.

3. Independent Motivations

If a tech platform wanted to assert that it is not a government agent for Fourth Amendment purposes, it could certainly argue that it has independent incentives to search for CSAM outside of helping law enforcement. After all, some courts explicitly consider this as a factor in the government agent analysis.[283] However, a court would likely find those incentives are not strong enough to induce the type of action the EARN IT Act would essentially mandate. Ultimately, if substantial independent incentives already existed, companies would have acted on them at some point in the last twenty years and obviated the need for the EARN IT Act in the first place. Even if tech companies are already

278. *See id.* at 606–12.
279. See *infra* Part V for further discussion.
280. *See supra* Part III.B (collecting and discussing cases in which courts have found no agency relationship between tech companies and the government in the CSAM context).
281. Lebron v. Nat'l R.R. Passenger Corp., 513 U.S. 374, 397 (1995).
282. *See supra* Part I.B(a).
283. *See supra* Part I.B.1.

inching in the right direction, the Act, and the accompanying legal exposure, would be a very strong tailwind.

Under the EARN IT Act, all companies would be encouraged to improve or develop methods to actively search for CSAM, invest more heavily in research, better support law enforcement, and train and support content moderators.[284] Additionally, because of the section 230 carve-out, the EARN IT Act would exert a potentially existential business threat on all tech companies in the form of civil and criminal investigations. For smaller firms with fewer resources, the pressure is likely to be even more intense. Moreover, the Commission's recommendations could essentially force them to adopt PhotoDNA and hire new employees to communicate directly with NCMEC and law enforcement. Many less visible companies, recognizing the minimal legal obligations they have today, do very little.[285]

Concededly, a court may be more likely to find independent motivation in cases involving highly scrutinized, public-facing platforms like Facebook because such platforms may have business reasons for scanning for CSAM. But even giants like Facebook and Google, which already implement PhotoDNA, would feel the pressure since the Act all but restricts their ability to change their polices outside of a zone of acceptability created by the Commission. The Commission's recommended actions may be socially beneficial, but they are likely to demand far greater commitment than firms have shown thus far. Surely a company acting to avoid a government-created threat of crushing litigation cannot be acting entirely independently.

Finally, it is important to remember that the mere presence of independent reasons for a private company's actions does not inoculate it from being found a government agency. After all, in *Skinner*, the railway line had its own reasons for drug testing its employees, but that did not stop the Court from concluding that it was a government agent.[286] Similarly, the Tenth Circuit in *Ackerman II* explained that an actor can have independent motivations while simultaneously working as an agent to a principal.[287]

In sum, tech companies complying with the EARN IT Act will likely satisfy the Fourth Amendment government agency tests. The Act is a clear example of the government strongly encouraging tech companies to take actions that they likely would not have taken otherwise. The Act also furthers a law enforcement objective—a "basic function[] of government."[288] But the government agency inquiry is only the beginning of the Fourth Amendment analysis. If courts decide

284. *See supra* Part I.B.1.

285. Dr. Farid Interview 2, *supra* note 107.

286. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989).

287. *See Ackerman II*, 831 F.3d 1292, 1302 (10th Cir. 2016). Still, some courts may place greater weight on this factor than *Ackerman* did. *See, e.g.*, United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003).

288. *See* Foley v. Connelie, 435 U.S. 291, 297 (calling law enforcement "one of the basic functions of government").

that tech companies act as agents of the government under the EARN IT Act, the searches or scans for CSAM conducted by those companies would be subject to Fourth Amendment scrutiny. Naturally, then, the next question is whether the CSAM-detection efforts spurred by the Act would run afoul of the Constitution.

V.
THE CONSTITUTIONALITY OF TECH COMPANIES' ACTIONS AS GOVERNMENT AGENTS UNDER THE EARN IT ACT

This Section continues the Fourth Amendment analysis from Part IV by asking whether tech companies' actions as government agents under the EARN IT Act would be constitutional. As *Skinner* explained, merely finding an agency relationship between a private party and the government does not end the Fourth Amendment analysis.[289] Whether action by the government violates the Fourth Amendment depends on two questions: 1) Is the government (or government agent) conducting a "search"? 2) If so, is that search "unreasonable"?[290] Typically, searches executed without a warrant are considered unreasonable.[291] This Section concludes that there are at least two plausible ways for courts to find tech companies' EARN IT-instigated scans for CSAM constitutional, thereby obviating the requirement for a warrant. Then, because of the novelty and potential complexity of cases arising out of the EARN IT Act or similar Congressional deputization of private companies, I suggest that Congress legislate more broadly on digital privacy.

Admittedly, it is difficult to predict how courts will rule on the Fourth Amendment question without specific facts about what the EARN IT Act's Commission will ask companies to do. This Section assumes that, at the very least, the EARN IT Act will result in all tech companies' adopting routine PhotoDNA scans of user email and chat messages, profiles, and cloud storage drives as standard practice. The analysis is mostly confined to such sweeping, warrantless, and suspicionless scans.

A. Is There a Fourth Amendment Search?

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and

289. *See Skinner*, 489 U.S. at 606–33 (analyzing, after finding an agency relationship, whether a Fourth Amendment search had occurred); *see also Ackerman II*, 831 F.3d at 1304 ("Assuming NCMEC is a governmental entity or agent, its actions still implicate the Fourth Amendment only if a 'search' took place . . . .").

290. *See Skinner*, 489 U.S. at 606–33.

291. Katz v. United States, 389 U.S. 347, 357 (1967) ("Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." (internal citations omitted)). Ultimately, however, the "touchstone of the Fourth Amendment is reasonableness" in light of all the circumstances. Ohio v. Robinette, 519 U.S. 33, 39 (1996) (internal quotes omitted).

seizures."[292] The Supreme Court has stated that a Fourth Amendment search occurs in two situations. A search occurs when "government officers violate a person's 'reasonable expectation of privacy.'"[293] A search also occurs when government officers "obtain[] information by physically intruding on a constitutionally protected area."[294] Because the subject matter of this Note does not involve physical trespass,[295] I only consider the reasonable expectation of privacy test below. For a court to find that a PhotoDNA scan of user messages and profiles qualifies as a Fourth Amendment search, the scan must violate a person's reasonable expectation of privacy.

The Fourth Amendment was written long before much of modern technology was even imaginable. Yet courts are increasingly forced to apply it in high-tech situations, thereby extending its meaning in intriguing ways.[296] In the face of this difficult task, courts and scholars are guided by the principle that the Fourth Amendment's protections should not be abrogated by new technology.[297] In this vein, the *Ackerman II* court reasoned that "an email is a 'paper' or 'effect' for Fourth Amendment purposes" because it can store not just private text, but photos and video as well.[298] The Sixth Circuit agrees. In its

---

292. U.S. CONST. amend. IV.

293. United States v. Jones, 565 U.S. 400, 406 (2012) (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

294. *Id.* at 406 n.3.

295. The idea of property rights in online data is not as outlandish as it may initially seem. We commonly discuss "our" data in everyday conversation, and the law is moving towards acknowledging the interest consumers have in what happens to the data they entrust to online service providers. *See* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation] (creating a landmark legal framework governing the collecting and processing of EU citizens' digital data); CAL. CIV. CODE § 1798.100–192 (West 2018) (California Consumer Privacy Act) (similar to the GDPR, creating a legal framework around Californian's digital data, including allowing users to opt out of the sale of personal data). Indeed, the *Ackerman II* court, speaking through now-Justice Gorsuch, opined that opening and viewing the contents of an email might constitute a Fourth Amendment "trespass." *Ackerman II*, 831 F.3d 1292, 1307 (10th Cir. 2016). For an in-depth discussion on the possibility of property rights in digital content outside of intellectual property, see Edina Harbinja, *Legal Nature of Emails: A Comparative Perspective*, 14 DUKE L. & TECH. REV. 227 (2015). For interesting, early examples of courts attempting to define property in a digital context, see United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (grappling with whether to define information stored on a computer as property); State v. McGraw, 480 N.E.2d 552 (Ind. 1985) (same); People v. Johnson, 560 N.Y.S.2d 238 (N.Y. Crim. Ct. 1990) (concluding that a stolen telephone credit card number written on a scrap piece of paper constituted property).

296. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (considering the applicability of the Fourth Amendment to thermal scanning technology); Unites States v. Jones, 565 U.S. 400 (2012) (GPS device); Carpenter v. United States, 138 S.Ct. 2206 (2018) (cell-tower location information).

297. *See Kyllo*, 533 U.S. at 34 (stating that technological advances should not "erode the privacy guaranteed by the Fourth Amendment"); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007, 1015–18 (discussing "technology neutrality"—the idea that the "degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world").

298. *Ackerman II*, 831 F.3d at 1304; *see* United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively

pathmarking decision in *United States v. Warshak*, it concluded that individuals have a reasonable expectation of privacy in their email communications.[299] Numerous courts have followed and extended this reasoning.[300] Conversely, some courts have concluded that email metadata, like to and from addresses or timestamps, are not protected, just as the outside of a letter or the participating numbers in a phone call are not protected.[301]

Courts, tech companies, and law enforcement officers appear to agree, in practice at least, that the logic behind this content versus metadata distinction likely extends to private messages on services like Facebook or WhatsApp, or even to cloud storage services like Apple's iPhotos or Google Drive.[302] But how does this distinction interact with PhotoDNA?

A PhotoDNA scan of private email or chat messages appears to fall in a gray area. Is the presence of child pornography within an email more like the

---

unreasonable."); *Ex Parte* Jackson, 96 U.S. 727, 732–33 (1877) (reasoning that letters should be treated "as if they were retained by the parties forwarding them in their own domiciles").

299. *See* 631 F.3d 266, 283–88 (6th Cir. 2010) (conceptualizing internet service providers as mail carriers and finding a Fourth Amendment privacy interest in the contents of emails, despite the fact that service providers had a contractual right to access the email's contents for certain purposes); *see also Ackerman II*, 831 F.3d at 1304 ("[I]f opening and reviewing 'physical' mail is generally a 'search' . . . why not 'virtual' mail too?").

300. *See, e.g.*, *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011) (relying on *Warshak* for the proposition that people have a protectable Fourth Amendment privacy interest in the contents of their emails); *United States v. Hanna*, 661 F.3d 271, 287 n.4 (6th Cir. 2011) (same); *In re U.S. for an Ord. Authorizing the Release of Hist. Cell-Site Info.*, 809 F. Supp. 2d 113, 124–25 (E.D.N.Y. 2011) (same); *Clements-Jeffrey v. Springfield*, No. 09-CV-84, 2011 WL 3207363, at *3 (S.D. Ohio 2011) ("[Warshak] can logically be extended to cover instant messages and webcam communications, the types of electronic communications at issue in this case."); *Coughlin v. Town of Arlington*, No. 10-10203, 2011 WL 6370932, at *10–11 (D. Mass. 2011) (relying on *Warshak* for proposition that emails are protected).

301. *See* United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2007) (finding no Fourth Amendment privacy interest in the email addresses of the senders or recipients of email messages); United States v. Keith, 980 F. Supp. 2d 33, 39–40 (D. Mass. 2013) ("There are some perhaps useful analogs from other methods of transmitting communications. So, for example, while there is not a reasonable expectation of privacy in the matter on the outside of a mailed envelope, there is as to the letter sealed inside, *see Ex Parte Jackson*, 96 U.S. 727, 733 (1877), and while there is not a reasonable expectation of privacy in the numbers dialed from a telephone, *see Smith v. Maryland*, 442 U.S. 735, 745 (1979), there is as to the conversation itself, *see Katz v. United States*, 389 U.S. 347, 352 (1967)."). For an excellent argument that metadata should *also* be protected by the Fourth Amendment, see Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 282–94 (2016).

302. *See Skinner*, 489 U.S. at 606-33 (citing relevant cases); *see also* Alexa Koenig, Keith Hiatt & Khaled Alrabe, *Access Denied? The International Criminal Court, Transnational Discovery, and the American Servicemembers Protection Act*, 36 BERKELEY J. INT'L L. 1, 28 n.137 (2018); Ira S. Rubinstein, Gregory T. Nojeim & Ronald D. Lee, *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIV. L. 96, 115 (2014) ("[S]ervice providers and the Justice Department now seem to agree that a judicial warrant is needed to compel third-party disclosure of content."); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1734 n.18 (2006) ("However, not all transmissions of data through third parties may count as conveyances to them for purposes of the third-party doctrine. Most significantly, the Court likely would not regard the content of calls and emails—as opposed to metadata such as time, date, and routing information as third-party data when obtained from telephone companies and ISPs rather than from their intended recipients.").

contents of the email, or more like the metadata of the email? That PhotoDNA can analyze the photos contained within a message is an argument for the former, but that PhotoDNA can scan for CSAM without reading the message is an argument for the latter. If the presence of CSAM is more analogous to metadata, then there is no search and we have no Fourth Amendment problem. If it is more analogous to content, then there may be a search.

The answer to this question could have serious practical consequences for the government and tech companies. PhotoDNA likely scans billions of photos every year for CSAM.[303] If a PhotoDNA scan counts as a Fourth Amendment search requiring a warrant, law enforcement efforts around CSAM could encounter a severe bottleneck. If such a scan is not a search, the question becomes a line-drawing one. What if tech companies, acting as government agents, scanned not just our photos, but our messages as well to find evidence of other crimes? Could computer algorithms be used to scan emails for messages relating to extremist ideology, drug trafficking, or terrorism?

Below, I consider two lines of Supreme Court cases which suggest that PhotoDNA scans, conducted on behalf of the government by tech companies, would be permissible under the Constitution. However, because of the massive constitutional implications of such a conclusion, I suggest that judges—or, ideally, Congress—carefully consider the limits of the government's ability to deputize tech companies before it goes too far.

1. Digital Dog Sniffs

This Section argues that one way courts may find PhotoDNA scans of private email or messages conducted by government-agent tech companies constitutionally permissible is by analogizing to drug-sniffing dogs. While the Supreme Court has never considered PhotoDNA in the Fourth Amendment context, it has considered the use of drug-sniffing dogs in certain circumstances. I believe a court could analogize to those cases when thinking about PhotoDNA scans.

In *United States v. Place*, the Court considered whether the use of a drug-sniffing dog on closed luggage in an airport constituted a search within the meaning of the Fourth Amendment.[304] It concluded that dogs are a "*sui generis*"—unique—exception to a typical search analysis because they could reveal the presence of contraband without revealing any other private information about the contents of the luggage to government officials.[305] The Court later interpreted the case as proposing that we have "no legitimate privacy interest" in contraband, so the dog-sniff could not logically count as a search and

303. *See* Smith, *supra* note 120.
304. 462 U.S. 696, 698 (1983).
305. *See id.* at 707.

therefore did not implicate the Fourth Amendment.[306] The Court came to a similar conclusion in *Illinois v. Caballes*, which concerned the use of a drug-sniffing dog during a routine traffic stop.[307] There too, the Court found that no Fourth Amendment search occurred because there is no legitimate privacy interest in possessing contraband.[308]

PhotoDNA scans are quite similar to drug-sniffing dogs. Since CSAM, like drugs, is contraband, we have no "legitimate privacy interest" in possessing it.[309] And, like drug-sniffing dogs, PhotoDNA operates within a binary framework. Just as a drug-sniffing dog can reveal the presence of contraband drugs in a purse or car trunk and nothing else, so too can PhotoDNA reveal the presence of contraband (CSAM) in digital communications without revealing the contents of the rest of the message. Indeed, PhotoDNA's nearly error-free performance far outstrips notoriously inaccurate drug-sniffing dogs.[310] This only strengthens the argument for the analogy.

Of course, the drug-sniffing dog cases mentioned above involved dog sniffs in public places, like airports or roadways. In another dog sniff case, *Florida v. Jardines*, the Supreme Court found a search when an officer brought a drug-sniffing dog onto private property.[311] Might a court find a similar infringement in a scan of a private message, a "paper or effect" under the Fourth Amendment, even though there is no analogous physical trespass? Another analogous Supreme Court case, *Kyllo v. United States*, suggests that the answer is likely no.[312]

Kyllo concerned the home, which, like a letter or email, is more intimate than an airport or traffic stop.[313] There, the Court found that the warrantless use of a thermal-imaging camera to detect the presence of an indoor marijuana grow lab was unconstitutional because it might have revealed additional details, no

306. United States v. Jacobsen, 466 U.S. 109, 123 (summarizing and interpreting *Place*'s analysis).

307. 543 U.S. 405, 406, 408–10 (2005) (first quoting *Jacobsen*, 466 U.S. at 123; and then quoting *Place*, 462 U.S. at 707).

308. *See id.* at 408–10.

309. *See Jacobsen*, 466 U.S. at 123 (noting that "this conclusion is dictated by [*Place*]").

310. *See also* Florida v. Harris, 568 U.S. 237, 243–50 (2013) (discussing the accuracy of drug-sniffing dogs and holding that their error rates do not change the probable cause analysis). *See generally Explosive-and Drug-Sniffing Dogs' Performance is Affected by Their Handlers' Beliefs*, U.C. DAVIS HEALTH (Feb. 23, 2011), https://health.ucdavis.edu/welcome/features/2010-2011/02/20110223_drug_dogs.html [https://perma.cc/Y3NA-ALJR]; Tadeusz Jezierski, Ewa Adamkiewicz, Marta Walczak, Magdalena Sobczyńska, Aleksandra Gorecka-Bruzda, John Ensminger & Eugene Papet, *Efficacy of Drug Detection by Fully-Trained Police Dogs Varies by Breed, Training Level, Type of Drug and Search Environment*, 237 FORENSIC SCI. INT'L 112, 114–15 (2014); Andrew E. Taslitz, *Does the Cold Nose Know? The Unscientific Myth of the Dog Scent Lineup*, 42 HASTINGS L.J. 15 (1990).

311. 569 U.S. 1, 11–12 (2013).

312. 533 U.S. 27 (2001).

313. *See Kyllo*, 533 U.S. at 31 ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." (internal quotations omitted)).

matter how trivial, about the interior of the suspect's home.[314] By contrast, PhotoDNA can do no such thing. Even though PhotoDNA has the ability to scan your most intimate messages and photos, the only detail it can reveal about you is whether or not you are attempting to transmit CSAM. Thus, even though PhotoDNA "looks" inside a traditionally protected Fourth Amendment space, it can only reveal that which we have "no legitimate privacy interest" in possessing anyway.[315] In the end, because the "touchstone of the Fourth Amendment is reasonableness" in light of all the circumstances,[316] courts could easily conclude that it is perfectly reasonable to automatically scan digital messages for CSAM using minimally invasive methods. Such a scheme seemingly has no immediate downside and could help protect children.

Still, there are nuances that complicate the analysis. The sheer scale of PhotoDNA's operation under the EARN IT Act must be taken into consideration.[317] Even if it can only detect contraband, it may be concerning to some that PhotoDNA could continuously scan nearly every image or video transmitted via the internet. If the post office hired an army of drug-sniffing dogs to inspect every single piece of mail for drugs, would that be reasonable under the Fourth Amendment?

Recall also that many tech companies engage human content moderators to uncover previously uncatalogued CSAM imagery.[318] What happens when content moderators, acting as government agents, access a user's profile or private messages for a more thorough search after a positive PhotoDNA match? What if they search through the contents of an entire private Facebook group after a photo in the group is flagged? The list of questions goes on. Thus, even if a PhotoDNA scan is constitutionally permissible under the drug-sniffing dog analogy, and even if the scale of the search were deemed reasonable, there are still difficult questions remaining about the ways in which content moderators and algorithms could potentially invade one's privacy. This could lead to a confusing array of court precedents that leave our digital privacy rights undefined.

---

314. *See id.* at 38 ("The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on.").

315. *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984).

316. *See* Ohio v. Robinette, 519 U.S. 33, 39 (1996).

317. *See* Carpenter v. United States, 138 S.Ct. 2206, 2220 (2018) (explaining that the sheer potential scale of using cell tower location data to track an individual's locations deserved special consideration). However, unlike in *Carpenter*, which involved a great deal of data about one person, mass PhotoDNA scans would involve a very tiny amount of data—whether CSAM is present—about millions of people's communications.

318. *See supra* Part II.B.

2. Third-Party Doctrine

A second way courts could approve PhotoDNA scans (and perhaps follow-on searches by content moderators as well) is the third-party doctrine. The third-party doctrine states that individuals have reduced privacy interests in information—such as phone numbers and bank deposit slips—they knowingly share with private companies.[319] Courts have only recently started to consider the third-party doctrine in the digital context. This Section argues that despite increased skepticism about the third-party doctrine, courts could apply it to approve PhotoDNA scans by tech companies acting as government agents.

Recent history suggests that courts might be less accepting of the doctrine than they once were. For example, in *Jones*, which concerned the Fourth Amendment ramifications of a GPS tracker placed on a suspect's vehicle, Justice Sotomayor wrote in her concurrence that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[320] She reasoned that the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[321]

The Court expressed further concern with the third-party doctrine in *Carpenter v. United States*. There, the Supreme Court held that the Fourth Amendment protected a defendant's cell tower location information, even though Carpenter had technically disclosed his location to a private party (his cell service provider).[322] The *Carpenter* Court framed its holding as declining to extend the third-party doctrine rather than eliminating it altogether, but the practical message it sent was clear: significant enough privacy concerns can override the third-party doctrine in some cases.[323] In *Carpenter*, the sheer volume of information the government could learn about the defendant's whereabouts through cell phone location data was highly concerning to the Court.[324] As such, it held the government needed a warrant to access that amount of information from a phone company, even though Carpenter's expectation was theoretically diminished because he had shared his location with his cell phone company by carrying his cell phone.[325]

---

319. *Carpenter*, 138 S.Ct. at 2219 (stating the rule); s*ee* United States v. Miller, 425 U.S. 435 (1976) (applying reasoning to bank deposit slips given to banks); Smith v. Maryland, 442 U.S. 735 (1979) (applying reasoning to phone numbers detected by a pen register).

320. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

321. *Id.*

322. *Carpenter*, 138 S.Ct. at 2219–21 (discussing the third-party doctrine and its inapplicability in the case).

323. *See id.* at 2220 (cautioning that the decision does not "disturb the application of *Smith* and *Miller"* or call "conventional" surveillance methods like security cameras into question).

324. *See id.* at 2217–19.

325. *See id.*

Similarly, in *Warshak*, the Sixth Circuit protected the content of an email notwithstanding the third-party doctrine.[326] Even in *Ackerman*, where AOL was not deemed a government agent, "the district court didn't rely upon third-party doctrine in ruling against Mr. Ackerman."[327] Instead, it assumed that Ackerman "had a reasonable expectation of privacy in his email."[328] All of this indicates that courts may be skeptical of the third-party doctrine in a digital context.[329]

But if the third-party doctrine *does* apply, and people do *not* have a reasonable expectation of privacy in the photos they send via tech companies, that raises another question: If the EARN IT Act converts tech companies into government agents, are they really third parties at all? Or are they a sort of a double agent—providing both a messaging service to users and a law enforcement service to the government? The court in *DiTomasso* approached this issue as a question of consent.[330] It ruled that the defendant had consented to AOL's government agent search because AOL included specific enough language about its cooperation with law enforcement in its terms of service; by contrast, the defendant had not consented to Omegle's government agent search because Omegle's terms were less clear.[331]

Professor Orin Kerr has also written about the relationship between consent and the third-party doctrine. He conceptualizes the third-party doctrine not as an application of the reasonable expectation of privacy test but as a doctrine of consent.[332] I take this formulation to mean that users who voluntarily transmit private information through a third party are consenting to the possibility that such information may be turned over to the government.

A terms-of-service solution derived from *DiTomasso* and Professor Kerr's consent idea might be simple, but would it be desirable? A Deloitte study found that over 90 percent of consumers agree to legal terms and services without reading them.[333] Even those who do read the terms often have no choice. Some tech platforms have monopoly power[334] and their apps and services, like the cell phones in *Carpenter*, are "almost a feature of human anatomy."[335] This

326. United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2011).

327. *Ackerman II*, 831 F. 3d 1292, 1305 (10th Cir. 2016).

328. *Id.*

329. *See* Thai, *supra* note 302, at 1744 (predicting the decline of the third-party doctrine).

330. United States v. DiTomasso, 56 F. Supp. 3d 584, 587 (S.D.N.Y. 2014).

331. *Id.* at 597–98. The district court took a similar approach on remand in *Ackerman*, reasoning that because Ackerman had agreed to AOL's terms of service, his subjective expectation of privacy in his email messages was not reasonable at the time of NCMEC's search. By violating AOL's terms, Ackerman opened himself up to the reporting actions AOL took. United States v. Ackerman (*Ackerman III*), 296 F. Supp. 3d 1267, 1271–73 (D. Kan. 2017), *aff'd*, 804 Fed. App'x. 900, 905 (10th Cir. 2020).

332. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588–90 (2009).

333. Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/FHJ8-AZ4H].

334. *See US Tech Giants Accused of 'Monopoly Power*,*'* BBC NEWS (Oct. 7, 2020), https://www.bbc.com/news/business-54443188 [https://perma.cc/QW4B-RT6E].

335. *See* Carpenter v. United States, 138 S.Ct. 2206,2218 (2018) (internal quotes omitted).

observation turns the concept of consent into a legal fiction. Perhaps it is reasonable to assume that people who use tech platforms implicitly consent to the idea that platforms might actively look for CSAM and report it to the police. But should someone be able to "consent" to other apparent constitutional violations like racial profiling or warrantless surveillance merely because they consented to a terms of service agreement? A consent-based framework seems to imply that the government can simply deputize tech companies into doing whatever it cannot do on its own then force them to change their terms and conditions to obtain their users' "consent."

Thus, while the third-party doctrine might supply a short-term solution to allow tech companies acting as government agents to continue scanning for CSAM, it is not a satisfying one to people concerned with Fourth Amendment protections and privacy.

B. What Next?

The possibility of tech companies acting as government agents in the ongoing fight against CSAM raises important and complex legal problems. This is primarily because Fourth Amendment jurisprudence, and the court system in general, has not kept up with modern technological developments. While I argued above that PhotoDNA scans conducted by tech companies acting as government agents would likely pass constitutional muster, it is far more difficult to predict the outcome—or even define the contours—of more complicated situations involving the mix of content moderators and software that the EARN IT Act may require. Moreover, Congress could use techniques similar to the EARN IT Act to potentially infringe on constitutional rights in other areas like terrorism or free speech. Obviously, given the ubiquitous nature of technology and tech platforms today, early decisions about such questions could very well define our society for years to come.

Just as important as the outcomes, however, is how courts arrive at them. Courts could analyze potential constitutional violations by government-agent tech companies through careful application of physical world precedents like the dog-sniff cases discussed above. Alternatively, they could adopt a blanket, consent-based doctrine that would result in consumers unwittingly contracting out of their constitutional rights by agreeing to a tech platform's terms of service. It would be difficult for courts to calibrate something in between that clearly and uniformly defines our Fourth Amendment rights online. Professor Erin Murphy phrased it well when warning that the courts' "expansive constitutionalization" of digital privacy could be "antidemocratic, antifederalist, piecemeal, incoherent, impracticably opaque, and inflexible (in that precedent is both easy to make and hard to dislodge)."[336]

336. Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 489 (2013).

Perhaps if Congress wants to wade into government agency waters with the EARN IT Act, it should also define clearly when it can and cannot conscript private tech companies into government service, and, accordingly, what our constitutional rights are with respect to digital privacy. For example, if consumers can consent to otherwise unconstitutional searches in a service agreement, Congress should put limits on which rights can be relinquished and which are too essential to be able to contract away. Congress is best suited for this because it has the power to hold hearings with stakeholders, gather data, and study the problem more deeply than a court can, and its work can set a baseline that states can build upon.

By criticizing section 230, proposing the EARN IT Act, and passing its predecessor, SESTA/FOSTA, federal elected representatives have already shown willingness to legislate in the digital realm.[337] Even some tech giants, like Google and Facebook, have broadly supported increased regulation as they face legal challenges implicating not only CSAM, but data privacy and election integrity as well.[338] These companies call for regulations with universal application, likely to avoid the patchwork regulations that would result from states and countries taking individual action.[339] Legislation may or may not be the appropriate approach in the CSAM context. One could argue that we should learn the pros and cons of various approaches by watching courts and state legislatures tackle the problem in different ways. But at least legislation provides the clarity and input from multiple voices that one-off judicial decisions cannot.

Precisely what a new legal framework around digital privacy and the use of tech companies as government agents should include is a topic for future scholarship. But suffice it to say that the EARN IT Act, or similar legislation,

---

337. *See supra* Part I.B.3 and accompanying notes.

338. Press Release, Mark Zuckerberg, Facebook, Big Tech Needs More Regulation (Feb. 18, 2020), https://about.fb.com/news/2020/02/big-tech-needs-more-regulation/ [https://perma.cc/ZP2D-WNY4]; Kent Walker, *How We're Supporting Smart Regulation and Policy Innovation in 2019*, GOOGLE BLOG: PUB. POL'Y (Jan. 8, 2019), https://blog.google/perspectives/kent-walker/principles-evolving-technology-policy-2019/ [https://perma.cc/WK3L-L3MU].

339. *See* Mark Zuckerberg, Opinion, *The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (Mar. 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html [https://perma.cc/9H2Q-NXNP] ("I also believe a common global framework — rather than regulation that varies significantly by country and state — will ensure that the Internet does not get fractured, entrepreneurs can build products that serve everyone, and everyone gets the same protections."). Indeed, some states have recently taken major regulatory action. Utah recently passed legislation requiring a warrant for certain electronic data stored with third parties like Google or Facebook. Molly Davis, *Utah Just Became a Leader in Digital Privacy*, WIRED (Mar. 22, 2019), https://www.wired.com/story/utah-digital-privacy-legislation [https://perma.cc/K8GV-NRHD]. California has also shown a willingness to legislate in the digital space with the California Consumer Privacy Act, a landmark consumer protection law modeled in part after the European General Data Protection Regulation. *See* General Data Protection Regulation, *supra* note 295; CAL. CIV. CODE § 1798.100–192 (West 2018). *See generally* Marianne Varkiani, *Comparing Privacy Laws: GDPR v. CCPA*, FUTURE OF PRIV. F. (Dec. 14, 2020), https://fpf.org/blog/comparing-privacy-laws-gdpr-v-ccpa/ [https://perma.cc/8CPV-UBCN] (comparing and contrasting the two laws).

could lead to some of the most hotly contested and nuanced Fourth Amendment inquiries in U.S. history.

CONCLUSION

At some point, we will have to decide as a country whether the level of digital privacy we enjoy today is worth the massive exploitation of children (and other criminal activity) that occurs online. Members of both political parties have shown great willingness to reel in tech companies, and section 230 protections have been at the center of most relevant discussions. While the EARN IT Act might successfully induce tech companies to do more to combat CSAM, the Act is also an unmistakable example of the government encouraging private entities to aid in a clear government function: law enforcement.

Applied properly, both Supreme Court precedent and state actor tests from various circuit courts support the conclusion that surveillance actions undertaken by tech companies under the EARN IT Act or similar legislation should be properly thought of as state action. While the Act might narrowly avoid violating the Fourth Amendment, consumers and legal professionals alike should be aware that legislation like the EARN IT Act would push the boundaries of Fourth Amendment jurisprudence.

Even if the EARN IT Act does not pass, it is only a matter of time before similarly ambitious legislation is proposed in Congress. If Congress passes such a bill, it should also decide on federal principles of online privacy more broadly. Otherwise, the courts will be left to create an ad hoc, patchwork body of digital privacy law that is neither consistent nor thorough and leaves unanswered important questions about child safety online.