PennState Dickinson Law

DICKINSON LAW REVIEW
PUBLISHED SINCE 1897

Volume 127 | Issue 1

Fall 12-18-2022

Scanning iPhones to Save Children: Apple's On-Device Hashing Algorithm Should Survive a Fourth Amendment Challenge

Timothy Gernand

Scanning iPhones to Save Children: Apple's On-Device Hashing Algorithm Should Survive a Fourth Amendment Challenge

Timothy Gernand*

ABSTRACT

When Apple announced it would combat the growth of child sexual abuse material (CSAM) on its platform by scanning all its users' devices without their consent, many of its loyal customers felt betrayed. With tech companies such as Google and Facebook arranging their business models around selling their customers' personal information, Apple customers saw the company's focus on privacy as a refreshing alternative. However, as Apple itself privately acknowledged, this emphasis on privacy had led to it becoming a haven for CSAM. Despite the reputational damage it would incur with its customers, Apple resolved to confront CSAM on its platform in an unprecedented manner. Until Apple's announcement, no major tech company had resolved to install a hashing algorithm directly onto its devices to search for CSAM.

Apple's move places itself in the middle of a legal firestorm with the protections of the Fourth Amendment squaring off against the public demand to eradicate CSAM and protect the nation's children from abuse. In deciding CSAM cases, courts have often focused on the application of the private search doctrine. Tech companies implementing anti-CSAM hashing protocols have sometimes run afoul of this doctrine and other aspects of Fourth Amendment jurisprudence.

This Comment argues that Apple's move not only complies with the constitutional standards expressed by circuit courts but exceeds those standards. In addition, a strong public policy justification exists for Apple's initiative. Congress has repeatedly expressed its intent to combat CSAM and protect children from sexual abuse, and by complying with this congressional intent,

* J.D. Candidate, Penn State Dickinson Law, 2023. I dedicate this Comment to my wife Kate for her ardent support and steadfast encouragement.

Apple aligns with public policy. Finally, this Comment recommends that the U.S. Supreme Court resolve the circuit split regarding Fourth Amendment-implicated CSAM cases by adopting a new rule.

TABLE OF CONTENTS

INTRODUCTION

> Do ye hear the children weeping, O my brothers,
> Ere the sorrow comes with years?
>
> They are leaning their young heads against their mothers, —
> And that cannot stop their tears.
>
> The young lambs are bleating in the meadows;
> The young birds are chirping in the nest;
>
> The young fawns are playing with the shadows;
> The young flowers are blowing toward the west—
>
> But the young, young children, O my brothers,
> They are weeping bitterly!
>
> They are weeping in the playtime of the others,
> In the country of the free.[1]

Child sexual abuse material (CSAM) is a worldwide scourge.[2] Historically, CSAM's impact was minimal, but the internet caused an explosion in supply and demand for this repulsive material.[3] Governments have struggled to respond effectively to the CSAM epidemic.[4] Faced with governments' lack of capability, private actors—including technology companies—have attempted to arrest

1. ELIZABETH BARRETT BROWNING, THE CRY OF THE CHILDREN (1844), *reprinted in* THE COLLECTED POEMS OF ELIZABETH BARRETT BROWNING 128 (Wordsworth Poetry Library 2015).

2. This Comment refers to "child sexual abuse material" (CSAM) because there is a broad movement away from the term "child pornography," as it is believed that the term "child pornography" connotes mere erotica, where CSAM emphasizes the exploitation involved in the crime's production. Michael Salter & Tyson Whitten, *A Comparative Content Analysis of Pre-Internet and Contemporary Child Sexual Abuse Material*, 43 DEVIANT BEHAV. 1, 1 n.1 (2021). CSAM is a "global child protection challenge and priority," with the United States reporting CSAM increasing at a rate of 50 percent per year. *Id.* at 1.

3. *See* Larissa S. Christensen et al., *The Theory and Evidence Behind Law Enforcement Strategies That Combat Child Sexual Abuse Material*, 23 INT'L J. POLICE SCI. & MGMT. 392, 393 (2021) (reporting that Australia, for example, catalogued an 80 percent increase in CSAM reports between 2017 and 2018).

4. *Id.*

the unprecedented growth of CSAM.[5] For example, Google and Facebook have played a key role in innovating anti-CSAM efforts.[6]

Apple, however, distinguished itself among the tech giants as the only large technology company that effectively championed privacy.[7] Although a highly successful marketing strategy, Apple's unqualified focus on privacy damaged its ability to confront CSAM on its platforms.[8] Belatedly recognizing that it had become a haven for child predators, Apple announced in 2021 that it would install a hashing algorithm to search for CSAM on all its devices.[9] After detecting CSAM, the images would be subject to human review before being referred to law enforcement.[10]

Apple's announcement revealed two things: (1) Apple was now willing to not only confront CSAM on its platform but to leapfrog its competitors by attacking CSAM in an unprecedented way, and (2) Apple would face significant criticism for abandoning its emphasis on privacy by degrading its users' device security.[11] Beyond these immediate revelations lies an important legal question: may a technology company scan its users' devices for CSAM without violating the U.S. Constitution?

The answer to that question requires a thorough analysis of the history of CSAM, the battle against it, and an analysis of the legal doctrines at play. The fallout from Apple's move has the potential

5. MaryJane Gurriell, *Born into Porn But Rescued by Thorn: The Demand for Tech Companies to Scan and Search for Child Sexual Abuse Images*, 59 FAM. CT. REV. 840, 841–42, 845 (2021) (describing the inability of government officials to arrest the growth of CSAM absent cooperation from tech companies, and the great success some companies have had in attacking CSAM on their platforms, including Facebook, Google, and Microsoft).

6. *Id.* at 845.

7. *See* Kif Leswing, *Apple Is Turning Privacy into a Business Advantage, Not Just a Marketing Slogan*, CNBC (June 7, 2021, 6:52 PM), https://cnb.cx/31h70SQ [https://perma.cc/WUP2-QK2N] (reporting Apple's privacy push since 2014).

8. *See* Sean Hollister, *Sweetheart Deals and Plastic Knives: All the Best Emails from the Apple vs. Epic Trial*, VERGE (Aug. 19, 2021, 10:00 AM), https://bit.ly/3B36kfG [https://perma.cc/Q5X7-HGNR] (providing via Number 71 an exchange between Apple executives in which one stated that Apple's weakness on CSAM was attributable to its strength on privacy).

9. Jon Porter, *Apple Scrubs Controversial CSAM Detection Feature from Webpage but Says Plans Haven't Changed*, VERGE (Dec. 15, 2021, 11:56 AM), https://bit.ly/34zufsL [https://perma.cc/H4S9-8HRB] (reporting that despite Apple scrubbing mention of its CSAM detection feature from its Child Safety webpage, Apple still plans to release the feature it first announced in August 2021).

10. *See also* APPLE, EXPANDED PROTECTIONS FOR CHILDREN FREQUENTLY ASKED QUESTIONS 5–6 (2021), https://apple.co/32FBf6A [https://perma.cc/6HHF-5EZ5] (stating that Apple will always conduct human review of flagged images before reporting to authorities).

11. *See* Lim, *infra* note 71; *see also* McKinney & Portnoy, *infra* note 75.

to impact Fourth Amendment jurisprudence in a significant way.[12] This Comment intends to illuminate a topic of grave importance to children, parents, Apple users, criminal defendants, and the legal community.

I. BACKGROUND

A. The Evolution of CSAM

1. Historical Background

The introduction of—and widespread access to—the internet has undeniable benefits for society. While writing letters was a favored way of communicating with loved ones in the past, the rise of technology applications like Facebook and Snapchat has made keeping in touch easier than ever before. Home chefs who in the past relied on passed-down recipes or borrowed recipe books can now quickly access a virtually limitless trove of meal ideas on Pinterest. While just two generations ago students researching a paper trudged to a library to acquire sources, today, they can access peer-reviewed journal articles and entire books from their smartphones.

Access to the internet has profoundly and likely irreversibly changed society, but not all this increased access to information has been positive. Fraudsters can now easily gain access to unwitting victims through phishing scams and exploitative emails.[13] Those involved with organized crime have been able to peddle their illicit wares more clandestinely via the virtually unregulated Darknet.[14] And, perhaps most devastating of all, the internet has allowed predators to quickly and easily acquire and distribute CSAM.[15]

---

12. *See* Lim, *infra* note 71. This inference arises from the combination of Apple's unique anti-CSAM initiative and the "growing tension in the circuits" over CSAM-related legal issues. *See id.* (illustrating the unique nature of Apple's NeuralHash algorithm); United States v. Wilson, 13 F.4th 961, 976 (9th Cir. 2021).

13. *See, e.g.*, Zainab Alkhalil et al., *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*, 3 FRONTIERS COMPUT. SCI. 1, 1 (2021) (defining phishing as "a highly effective form of cybercrime that enables criminals to deceive users and steal important data").

14. *See* Mihnea Mirea et al., *The Not So Dark Side of the Darknet: A Qualitative Study*, 32 SEC. J. 102, 103 (2019) (characterizing the Darknet as an illegal drug haven and source of identity theft schemes).

15. *See* Diane Jennings, *Fight Against Child Pornography an Uphill Battle in the Internet Age*, DALL. MORNING NEWS (July 28, 2013), https://bit.ly/3EdizYW [https://perma.cc/5S7E-CSRD] (reporting that while CSAM had been mostly eradicated in the 1980s, the National Center for Missing & Exploited Children now receives 10,000 CSAM tips per week and 91 million CSAM images have been seized by authorities since 2002, but in contrast, only 5,000 people were arrested for CSAM-related crimes in 2009).

Prior to the advent of the internet, would-be CSAM viewers were unable to organize in any meaningful way because it was difficult to find access to the desired resources anonymously.[16] A child predator could not simply ask a Blockbuster associate their recommendations for an illegal pornographic video of prepubescent children or invite their neighbors for a CSAM viewing party without quickly gaining unwanted attention from law enforcement.[17] Small groups of like-minded deviants certainly existed, but their ability to readily access their desired materials was limited.[18] In fact, prior to the ubiquity of internet access, CSAM was not regarded as a significant problem by academics.[19] While some producers of child pornography in the 1970s distributed their sexually explicit materials via the mail system, by the 1980s, law enforcement considered widespread sexually explicit material virtually eradicated.[20]

2. The Tech Boom

When internet access exploded in the late 1990s and early 2000s, the amount of CSAM available increased proportionately.[21] The ability to share and receive illicit pornographic content quickly, easily, and relatively anonymously via the internet led to significant increases in the volume of child-focused sexual content in the past two decades.[22] Between 1998 and 2018, the number of reported images of CSAM increased more than 613,233 percent.[23] A 2021 study by the U.S. Sentencing Commission revealed even more troubling statistics about the nature of this content.[24] In 2019, more

16. *See id.*
17. *See id.*
18. *See id.*
19. *See* Salter & Whitten, *supra* note 2, at 1–3 (describing the skepticism of academics toward CSAM and its negative effects on society until the digital evidence of CSAM provided by the internet undermined skeptics' positions).
20. *Id.*
21. U.S. DEP'T OF JUST., CHILD PORNOGRAPHY (2020), https://bit.ly/3nrNppU [https://perma.cc/N7DE-X6Q9] (last visited Oct. 30, 2021) (describing the parallel between the rise of the internet and the rise of CSAM, and preferring the terms "child sexual exploitation" and "child sexual abuse" to the legacy term "child pornography" because the term "child pornography" does not adequately capture the extent of damage inflicted on children).
22. *See id.*
23. *See* 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://nyti.ms/3pvQyaW [https://perma.cc/P4L6-VRXE] (tracking the progression of reported CSAM from 3,000 reports in 1998 to 18.4 million in 2018, with the 2018 reports including a total of 45 million CSAM images).
24. *See* U.S. SENT'G COMM'N, FEDERAL SENTENCING OF CHILD PORNOGRAPHY: NON-PRODUCTION OFFENSES 1–3 (2021), https://bit.ly/3jxRubc [https://perma.cc/D5VR-XUMA].

than 50 percent of the millions of illicit images discovered from CSAM-related investigations featured toddlers and infants.[25] The FBI also disclosed that in 2019 there were numerous sites on the Darknet devoted exclusively to sexualized images of very young children.[26] One such site generated more than 150,000 unique users within 2 months of it being operational.[27] These statistics point to a horrific scale of child abuse that would have been difficult to imagine from the standpoint of CSAM's nadir in the 1980s.

B. The Battle Against CSAM

1. The Government Outmatched

Law enforcement agencies have attempted to identify and charge CSAM perpetrators but, despite some successes in prosecuting larger networks of CSAM consumers and distributors, combatting CSAM access in a meaningful way has proven difficult.[28] Despite having entire teams of law enforcement personnel in dozens of countries working exclusively on child exploitation-related crimes and investing billions of dollars on this issue, the number of CSAM images has substantially increased.[29] As CSAM images proliferate, law enforcement agencies have struggled to disrupt the more organized and covert pedophile networks.[30] Some of these groups even provide guides on how to avoid law enforcement attention by using specific encryption techniques, coded language, and sharing files via less traditional fora like online gaming platforms.[31]

2. The Public Takes Action

Given the unique vulnerability of children and the lifelong negative effects of their sexual exploitation, the public has a significant

---

25. *Id.* at 4.

26. *See FBI Budget Request for Fiscal Year 2020: Hearing Before the Subcomm. on Com., Just., Sci. & Related Agencies of the H. Appropriations Comm.*, 116th Cong. (2019) (statement of Christopher Wray, Director, Federal Bureau of Investigation), https://bit.ly/3pwKbUV [https://perma.cc/WXS5-ZVTW].

27. *Id.*

28. *See* Patrick Smith & Carlo Angerer, *Dark Web Child Abuse Image Site with 400,000 Members Taken Down in Global Police Sting*, NBC NEWS (May 3, 2021, 10:08 AM), https://nbcnews.to/3Gfg0rb [https://perma.cc/N3KG-UDXA] (portraying dark web CSAM communities as demonstrating "resilience" to law enforcement operations).

29. *See* Keller & Dance, *supra* note 23.

30. *See* U.S. DEP'T OF JUST., *supra* note 21 (representing that CSAM is available through "virtually every Internet technology" and that offenders use "increasingly sophisticated" methods to evade law enforcement).

31. *Id.*

interest in ensuring their protection.[32] Finding the children used in pornographic content is considered particularly critical as sexualized images are often not the only abuse these children suffer.[33] In fact, there is a well-established connection between CSAM and broader sexual violence.[34]

The inability of law enforcement agencies to significantly hamper CSAM has prompted a variety of concerned stakeholders to become more involved in combatting this particularly vile form of criminality.[35] In the United States, the group Perverted Justice gained widespread attention for their involvement in the Dateline "To Catch a Predator" series, while Canadian civilians created a similar group called Creep Catchers.[36]

Private companies, particularly those directly involved with the internet, have also implemented policies designed to reduce child exploitation-related offenses.[37] Popular social media platforms like Facebook, Instagram, and Twitter provide users with options to report sexually explicit content directly to moderators.[38]

Unfortunately, because the COVID-19 pandemic led to children spending more time at home, reports of pornographic images of minors more than doubled, leaving the platforms unable to meet

---

32. Ateret Gewirtz-Meydan et al., *The Complex Experience of Child Pornography Survivors*, 80 CHILD ABUSE & NEGLECT 238, 242–43 (2018) (indicating that nearly half of adult survivors of child pornography experienced guilt, shame, ongoing vulnerability, and fear they would be recognized due to the images' widespread distribution).

33. *See* U.S. DEP'T OF JUST., *supra* note 21 (reporting an increase in images depicting sadistic and violent child sexual abuse).

34. *See* Candice Kim, *From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*, AM. PROSECUTORS RSCH. INST., NAT'L CTR. FOR PROSECUTION OF CHILD ABUSE 1 (2004), https://bit.ly/2Zx4zua [https://perma.cc/J7EP-QTD7] (reporting that a substantial number of arrested child pornographers were confirmed child molesters and that a majority of CSAM-related offenders admitted to physical sex crimes).

35. *See* Brend, *infra* note 36; *see also* Solon, *infra* note 37.

36. Yvette Brend, *Perverting Justice? Privacy Ruling Won't Stop Vigilantes 'Addicted' to On-Camera Stings*, CBC NEWS (July 29, 2017), https://bit.ly/3jPjDKS [https://perma.cc/3ZPP-BZHA] (reporting that despite a ruling against the British Columbia-based Creep Catchers, the group intended to continue preventative efforts to stop CSAM).

37. Olivia Solon, *Child Sexual Abuse Images and Online Exploitation Surge During Pandemic*, NBC NEWS (Apr. 23, 2020, 3:01 PM), https://nbcnews.to/3nFeJkV [https://perma.cc/623J-FWTR] (reporting that Zoom now defaults to password protection for meetings because of CSAM reports, that many other technology companies have zero-tolerance policies for CSAM, and that locating and removing such content is a top priority).

38. *Id.* (indicating that technology companies have automated systems in place to target CSAM but these systems are inadequate, forcing these companies to rely heavily on user reports to identify and remove CSAM).

the demand for increased scrutiny.[39] Some strategies undertaken by these businesses have proven more successful than others. For example, when Google and Bing implemented warnings that searches for CSAM were illegal and recommended that the searcher seek help, one study found a 67 percent decrease in the number of CSAM searches in the United States.[40] This statistic demonstrates how warnings may play a significant role in deterring potential CSAM viewers from seeking illicit content and may provide a justification for other powerful technology companies to utilize similar practices.

3. The National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children (NCMEC) is a nonprofit organization that plays a key role in Big Tech anti-CSAM efforts.[41] In 1984, John and Revé Walsh founded NCMEC in response to the tragic kidnapping and murder of their six-year-old son, Adam.[42] John and Revé Walsh's purpose in founding NCMEC was to improve the disorganized, fragmented, and ultimately ineffective law enforcement response they witnessed during their son's disappearance.[43] Over time, NCMEC evolved into the premier nonprofit organization dealing with missing and exploited children's issues.[44] Today, NCMEC employs over 340 people who work to prevent child exploitation and to help find missing children.[45]

NCMEC is not merely a nonprofit organization with substantial credibility in the CSAM space.[46] Instead, it is an organization

---

39. *Id.*

40. Thanh Ly et al., *Understanding Online Child Sexual Exploitation Offenses*, 18 CURRENT PSYCHIATRY REPS. 74, 74 (2016).

41. *See* NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, ABOUT Us, https://bit.ly/3psEJCz [https://perma.cc/K4RP-J2UU] (last visited Oct. 30, 2021) [hereinafter NCMEC]; *see also* NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, 2020 REPORTS BY ELECTRONIC SERVICE PROVIDERS (ESP) (2021), https://bit.ly/3zqkvxC [https://perma.cc/5BR6-5RX9] [hereinafter NCMEC REPORTS] (describing how dozens of ESPs use NCMEC to report CSAM on their platforms).

42. *See 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. 1 (2020) (statement of John Shehan, Vice President, National Center for Missing & Exploited Children), https://bit.ly/3jr3tHh [https://perma.cc/9QLR-5AYB].

43. *See id.*

44. *Id.*

45. *Id.*

46. *See* 34 U.S.C. § 11293(b) (providing for an annual grant of federal funds to NCMEC to operate reporting services for CSAM and other activities); *see also*

that the U.S. Congress chose to both receive federal funding and play a principal role in the federal government's anti-CSAM campaign.[47] Showcasing the power that Congress invested in NCMEC (and perhaps also its quasi-deputization as a law enforcement entity), service providers that fail to report CSAM on their platforms to NCMEC violate federal law.[48] However, service providers are not required to search for CSAM on their platforms; the duty to report is only triggered if and when service providers discover CSAM.[49]

NCMEC maintains the CyberTipline, a centralized reporting system for online CSAM that received 21.7 million reports in 2020 from dozens of Electronic Service Providers ("ESPs").[50] It is worth noting, of those 21.7 million reports, approximately 20.3 million originated from Facebook, while only 265 originated from Apple.[51] This massive disparity between reports from the two companies is almost certainly a result of underreporting by Apple due to its technical inability, or refusal, to confront CSAM on its platform, rather than an actual indication of the difference in CSAM prevalence on the two platforms.[52] For years, Facebook has actively scanned every photo uploaded to its platform for CSAM, while Apple, despite having the capacity to do the same, has—until recently—refrained from doing so.[53] Presumably, Apple's reports to NCMEC are limited because it only began to scan its iCloud Mail service in 2019,

18 U.S.C. § 2258A (providing that ESPs have a duty to report CSAM on their platforms to NCMEC).

47. *See* 34 U.S.C. § 11293(b); *see also* 18 U.S.C. § 2258A.

48. 18 U.S.C. § 2258A(a)(1)(A).

49. *See id.*

50. NCMEC REPORTS, *supra* note 41.

51. *Id.*

52. *Compare* Antigone Davis, *New Technology to Fight Child Exploitation*, FACEBOOK (Oct. 24, 2018), https://bit.ly/30U23yS [https://perma.cc/LGA8-KZH7] (describing that in 2018, Facebook had already been using photo-matching technology "for years" to detect and report CSAM on its platform, and that it was currently upgrading to machine learning technologies to be able to not only detect CSAM at the time of upload but to predict which accounts would upload CSAM), *and* FACEBOOK TRANSPARENCY CENTER, POLICY ON CHILD SEXUAL EXPLOITATION, https://bit.ly/3nmLFOT [https://perma.cc/6WM7-TRRE] (last visited Oct. 23, 2021) (describing Facebook's practice of removing even well-intentioned nude pictures of children posted by parents), *with* Ben Lovejoy, *Apple Already Scans iCloud Mail for CSAM, but Not iCloud Photos*, 9TO5MAC (Aug. 23, 2021, 4:43 AM), https://bit.ly/2ZqT5bP [https://perma.cc/BET2-YYUM] (reporting that Apple began scanning iCloud Mail for CSAM in 2019, but did not scan iCloud Photos despite iCloud Photos' lack of encryption and Apple's ability to scan).

53. *See supra* note 52 and accompanying text.

and its planned expansion of CSAM detection on iCloud Photos will result in a massive increase in reports to the CyberTipline.[54]

C. Anti-CSAM Efforts

1. Historical Background

Early efforts to address the online CSAM problem faced two primary obstacles: legal roadblocks and technological deficiencies.[55] Governments were confounded by legal issues such as determining whether an act constituted "child pornography" and whether an apparent minor was old enough to trigger a relevant legal provision.[56] Police struggled to deal with even rudimentary forms of encryption such as encrypted emails and internet protocol ("IP") masking, which prevented police from geolocating a CSAM suspect.[57]

A Facebook-integrated application developed by a United Kingdom government agency and implemented in 2010 both exemplified an early form of technology that could succeed against CSAM and presaged the future role of public-private partnerships in combatting CSAM.[58] The application provided users a simple way to report CSAM or attempts to groom children, and within a month of introduction resulted in 211 reports, many of which could result in serious criminal charges.[59] While somewhat effective, this technology has limited use in combatting CSAM on a wide scale because it is simply impossible for human-initiated reports to ever amount to more than a tiny fraction of the tens of millions of CSAM images transmitted annually.[60]

---

54. *See* NCMEC REPORTS, *supra* note 41. The inference that Apple's new tools will lead to a large increase in reports to NCMEC arises from comparing Facebook's 20.3 million reports to the CyberTipline in 2020, Google's 546,704 reports, and Amazon's 2,235 reports, with Apple's paltry 265 reports, despite Apple holding 52 percent of the smartphone user market in the United States. *Id.*; *see also* STATISTA, SUBSCRIBER SHARE HELD BY SMARTPHONE OPERATING SYSTEMS IN THE UNITED STATES FROM 2012 TO 2021 (2021), https://bit.ly/3ptpR6L [https://perma.cc/Z6FB-DD92] (reporting Apple's share of the smartphone user market rose from 29.5 percent in January 2012 to 52 percent in May 2021).

55. *See* Anne Burke et al., *Child Pornography and the Internet: Policing and Treatment Issues*, 9 PSYCHIATRY, PSYCH. & L. 79, 80 (2002).

56. *See id.*

57. *See id.*

58. *See* Mark Sweney, *Facebook ClickCeop App to Offer Optional 'Panic Button,'* GUARDIAN (July 12, 2010, 2:00 AM), https://bit.ly/3Ewxm1i [https://perma.cc/CN9H-TVWU].

59. *See* Jemima Kiss, *Facebook Child Protection App Prompts 211 Reports of Suspicious Online Activity*, GUARDIAN (Aug. 12, 2010, 11:26 AM), https://bit.ly/3bo3Z4r [https://perma.cc/XY7R-HLNU].

60. *See* Keller & Dance, *supra* note 23.

2. Hashing

As online CSAM has grown exponentially from its early days, new technologies have formed to combat the surge of illegal material. One such technology is hashing.[61] A hash value is a set of characters generated by a mathematical algorithm and derived from an image that allows computer programs to quickly scan the content of many images by simply reading the set of characters.[62] Hashing refers to the technique of generating these hash values and using them to analyze media data.[63]

Hashing has become the preferred anti-CSAM technique of technology companies and law enforcement because it allows for the rapid scanning of large volumes of images and for the verification that an apparent copy of an image is in fact an exact copy of the original image.[64] For example, instead of requiring the computing power necessary to scan and compare a relatively large image file of purported CSAM to an image file of known CSAM, hashing allows for the comparison of two relatively small strings of characters. By reducing the size of the scanned files, hashing results in more efficient computer processing of suspect images.[65] Perhaps more importantly, using hashing to search for CSAM does not require human input.[66] Removing the human element *during the search* is critical for efficient processing for CSAM searches; however, it is just as critical to retain the human element *after the search* to meet the legal standard of the private search doctrine.[67]

---

61. United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) (citing Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38–40 (2005)).

62. *See* Salgado, *supra* note 61, at 38–40.

63. *Id.*

64. *Id.*

65. *Id.* at 40 (describing how hashing can automate the previously massive analytical task of comparing large numbers of images).

66. *Id.*

67. Companies should retain the human element after an automated search is completed because although some circuit courts have found hashing's discovery of CSAM to be equivalent to a human's discovery of CSAM, other circuit courts have rejected this equivalency and insist on a human to satisfy the private search exception. *See* United States v. Wilson, 13 F.4th 961, 978 (9th Cir. 2021) (discussing the Ninth Circuit's differing interpretation of the private search doctrine with the Fifth and Sixth Circuits and noting that "no human had viewed Wilson's images before").

D. Apple's Anti-CSAM Move

1. Apple's Announcement

In August 2021, Apple announced its intention to prevent the spread of CSAM via a software update that would: (1) apply new forms of cryptography, (2) provide new communication tools, and (3) update its Siri and Search tools.[68] The relatively innocuous and uncontroversial second and third parts of Apple's plan do not implicate any legal doctrine, and this Comment will not address them.[69] However, Apple's announced new forms of cryptography involve the unprecedented installation of CSAM hashes onto every Apple device with the aim of scanning every photo uploaded to iCloud for matches to known CSAM hashes.[70] While other technology companies have used hashing for years to disrupt CSAM on their platforms by scanning emails and cloud data, no major technology company has yet admitted to a plan to install anti-CSAM hashing technology directly onto users' devices.[71]

Apple apparently recognized, likely due to its failure to confront CSAM on its platform relative to the efforts made by Big Tech competitors such as Facebook and Google, that it had become a favored platform for distributing CSAM.[72] Apple's own anti-fraud chief, Eric Friedman, stated in a private conversation that

---

68. *See* APPLE, EXPANDED PROTECTIONS FOR CHILDREN, https://bit.ly/3IRF1K0 [https://perma.cc/GW5N-NRJ4] (last visited Mar. 6, 2022) (displaying the page as it existed on October 25, 2021, before it was updated to remove mention of Apple's CSAM detection tools); *see also* Joanna Stern, *Apple's Child-Protection Features and the Question of Who Controls Our Smartphones*, WALL ST. J. (Aug. 13, 2021, 12:44 PM), https://on.wsj.com/3CLq8pt [https://perma.cc/J3YL-S774].

69. *See* APPLE, *supra* note 68. Apple's "new communication tools" refer to updates to iMessage that include blurring sexually explicit photos and notifying parents when children send or receive such photos, and the Siri and Search updates involve warnings when users search for CSAM, like those warnings used by Google and Bing and discussed in note 22. *Id.*; *see also* Ly, *supra* note 40.

70. *See* APPLE, CSAM DETECTION: TECHNICAL SUMMARY 4 (2021), https://apple.co/31nFiU1 [https://perma.cc/R7AZ-BVTV].

71. *See* Swee Kiat Lim, *Apple's NeuralHash—How It Works and How It Might Be Compromised*, TOWARDS DATA SCI. (Aug. 20, 2021), https://bit.ly/3GR7gIj [https://perma.cc/QX2R-QCJZ] (describing Apple's NeuralHash technology featuring client-side scanning as "new" and possessing both capabilities and vulnerabilities that are unique relative to server-side anti-CSAM hashing technologies utilized by Bing, Google, Facebook, etc.); *see also* EDUCATED GUESSWORK, PERCEPTUAL VERSUS CRYPTOGRAPHIC HASHES FOR CSAM SCANNING (Aug. 24, 2021), https://bit.ly/2YctH98 [https://perma.cc/LX9M-X4XK] (contrasting Apple's NeuralHash technology with other technology companies' use of the competing algorithm PhotoDNA and discussing the exposure risk inherent in NeuralHash's client-based algorithm because users will have access to the algorithm on their devices).

72. *See* Hollister, *supra* note 8 (providing via exchange Number 71 an iMessage conversation where Apple's anti-fraud chief Eric Friedman states that

"we [Apple] are the greatest platform for distributing child porn."[73] Friedman attributed this failure to Apple's focus on privacy, an area in which he alleged Apple's rivals underperformed.[74]

2. The Backlash and Apple's Response

Privacy, the concept that Apple repeatedly touted as its greatest strength in marketing campaigns, was on the minds of Apple's critics, who strongly contested Apple's plan to implement cryptographic tools requiring the installation of hashes onto every Apple device.[75] One critic decried Apple's move as the installation of a "back door" that would enable nefarious actors to prey on users' personally identifiable information and present an opportunity for authoritarian governments to spy on dissidents' communications.[76] Edward Snowden declared that Apple's anti-CSAM tools represented "mass surveillance" and turned users' iPhones into "iNarcs."[77]

Apple responded to the controversy by announcing that it would delay by "months" the implementation of its anti-CSAM hashing protocol.[78] Despite its willingness to postpone installing its hashing protocol on devices, there is no indication that Apple will not fully implement it.[79]

E. Fourth Amendment Implications

Apple's new cryptographic tools may implicate the Fourth Amendment. The Fourth Amendment, in relevant part, provides, "[t]he right of the people, to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall

---

Apple has deliberately avoided acknowledging the CSAM problem on its platform and when Apple does acknowledge it, Apple underreports the problem).

73. *Id.*

74. *See id.*

75. *See* Leswing, *supra* note 7 (reporting Apple's privacy push since 2014); *see also* Jeff Parrott, *Apple Says It Will Scan iPhones for Images of Child Abuse, But Is That a Breach of Privacy?*, DESERET NEWS (Aug. 6, 2021, 1:22 PM), https://bit.ly/3xGfsqD [https://perma.cc/T7SW-RGBZ]; Edward Snowden (@Snowden), TWITTER (Aug. 5, 2021, 10:23 PM), https://bit.ly/3EdRntE [https://perma.cc/DG76-36MQ]; India McKinney & Erica Portnoy, *Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life*, ELEC. FRONTIER FOUND. (Aug. 5, 2021), https://bit.ly/32PGmkt [https://perma.cc/W8UG-QXM5].

76. McKinney & Portnoy, *supra* note 75.

77. Snowden, *supra* note 75.

78. APPLE, *supra* note 68 (updating the original page on September 3, 2021 to include a comment announcing the delay).

79. *Id.* (describing the delay as one undertaken to improve the product "before releasing" it); Porter, *supra* note 9.

not be violated."[80] By a plain reading of the Fourth Amendment, it may appear that running searches on one's device without permission could be construed as an unreasonable search in violation of the Fourth Amendment. However, a rich history of Fourth Amendment jurisprudence provides several considerations when evaluating Apple's move, including the development of the private search doctrine and contemporary Fourth Amendment decisions involving CSAM, NCMEC, and technology companies.[81]

1. Pre-Private Search Doctrine

In the early years of the communication revolution sparked by the adoption of the telephone in the United States, the Supreme Court took a dim view of criminal defendants' Fourth Amendment-based objections to government wiretapping.[82] In the Supreme Court case of *Olmstead v. United States*,[83] the majority reasoned that a warrantless government wiretap of a defendant was legal because there was "no searching" and "no seizure."[84] In seeing wiretapping as intangible evidence secured only by "hearing," the Court appeared to connect wiretapping to the common law's conception of eavesdropping, which was considered a mere nuisance.[85] Under an *Olmstead* view of the Fourth Amendment, one's intangible effects are not entitled to the same protection as one's tangible effects.[86]

In a case that would set the stage for later private search doctrine disputes, the Supreme Court held in *Burdeau v. McDowell*[87] that the Fourth Amendment does not protect an individual from a private party stealing one's effects and then handing them over to the government.[88] In a sense, evidence that would have been illegal for the government to obtain in such a manner is "cleansed" by a

80. U.S. CONST. amend. IV.

81. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 270–361 (7th ed. 2021) (discussing at length the development of Fourth Amendment jurisprudence and the private search doctrine).

82. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (stating that one who installs and uses a telephone in his house, intending to transmit his voice outside of his home, loses Fourth Amendment protections for any message transmitted with this telephone).

83. 227 U.S. 438 (1928).

84. *Id.* at 464.

85. *Id.*; *see also* SOLOVE & SCHWARTZ, *supra* note 81, at 277 (detailing the understanding of eavesdropping at common law).

86. *See* SOLOVE & SCHWARTZ, *supra* note 81, at 282 (concluding that *Olmstead* led to a view that Fourth Amendment protections are only available to defendants who suffer a physical trespass).

87. 256 U.S. 465 (1921).

88. *See id.* at 475–76.

private party's first obtaining the evidence, even if the private party steals property.[89] The Court's reasoning relied on a literal interpretation of the Fourth Amendment as proscribing only government action.[90] The *Burdeau* Court's holding raises an ethical issue: if the government is forbidden from acting, but a private party is not forbidden from acting on behalf of the government, is there not an incentive for the government to deputize the private party to circumvent the law on its behalf?[91]

In *Lopez v. United States,*[92] Justice Warren provided the first warning that the Supreme Court could conceivably go too far in limiting the reach of the Fourth Amendment, writing that "advances in the field of electronic communication constitute a great danger to the privacy of the individual."[93] However, *Lopez* continued the trend of placing limits on Fourth Amendment protections by establishing that the government does not violate the Fourth Amendment when it warrantlessly records a conversation between a police informant and a suspect.[94]

Reversing the trend of pro-government decisions, in *Katz v. United States*,[95] the Supreme Court held that "searches conducted outside the judicial process, without prior approval by a judge, are *per se* unreasonable under the Fourth Amendment."[96] Justice Harlan's concurrence in *Katz* was noteworthy because it provided a two-part test to establish whether Fourth Amendment protections apply.[97] First, a person must exhibit an "actual (subjective) expectation of privacy," and second, that expectation must be reasonable.[98] This test would later become known as the "reasonable expectation of privacy test."[99]

After setting limits on the government's ability to engage in warrantless searches, the Supreme Court emphasized that the

89. *See id.*; *see also* United States v. Wilson, 13 F.4th 961, 967–68 (9th Cir. 2021) (detailing at length the impact of *Burdeau* on Fourth Amendment jurisprudence).

90. *See Burdeau*, 256 U.S. at 475 (concluding that the Fourth Amendment was intended only as a restraint on sovereign authority).

91. *See id.* at 476 (Brandeis, J., dissenting) (allowing for the constitutionality of the majority's opinion while protesting its result as violating the rule of law and common decency).

92. 373 U.S. 427 (1963).

93. *Id.* at 441 (Warren, J., concurring).

94. *Id.* at 438–39 (majority opinion) (extending the holding in *Olmstead* by relying on a physical interpretation of Fourth Amendment protections).

95. 389 U.S. 347 (1967).

96. *Id.* at 357.

97. *Id.* at 360–61 (Harlan, J., concurring).

98. *Id.*

99. SOLOVE & SCHWARTZ, *supra* note 81, at 292.

Fourth Amendment should not restrict private parties from voluntarily reporting crimes to the police.[100] In *Coolidge v. New Hampshire*,[101] the Court held that a defendant's Fourth Amendment rights were not violated when his wife, under her own volition, provided police with evidence implicating him in a murder.[102] The Court's relevant inquiry was whether, in providing evidence to the police, the private party acted under government compulsion.[103] When presented with incriminating evidence freely given to them by a cooperating witness, police should not be required to "avert their eyes."[104]

The Supreme Court extended *Coolidge* further in *United States v. Miller*,[105] in which the government's conduct in directing a bank to maintain and report customer records to the government was held constitutional.[106] Despite the government's effective deputization of a private party for law enforcement purposes, the majority did not see any Fourth Amendment implication in the government's conduct.[107] The Court reasoned that the government's intrusion into private records was constitutional because the search did not intrude on a "zone of privacy" involving a person or property in a constitutionally protected area.[108]

2. The Private Search Doctrine

The private search doctrine plays a significant role in nearly every CSAM-related Fourth Amendment case.[109] This doctrine permits the government to obtain evidence under circumstances that would otherwise require a warrant.[110] When a private party first

100. *See* Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971).
101. 403 U.S. 443 (1971).
102. *Id.* at 486.
103. *Id.* at 489.
104. *Id.*
105. 425 U.S. 435 (1976).
106. *Id.* at 440.
107. *Id.*
108. *Id.*
109. *See* United States v. Wilson, 13 F.4th 961, 967–68, 976–79 (9th Cir. 2021) (detailing the evolution of the private search doctrine and other appellate courts' interpretations of the doctrine). The third party doctrine is a related but separate legal doctrine that has yet to emerge as a significant factor in CSAM-related Fourth Amendment cases. *Id.* The third party doctrine allows the government to use information obtained by third parties, even information obtained in confidence, in a criminal prosecution without violating the Fourth Amendment. *Miller*, 403 U.S. at 443. *United States v. Ackerman* hinted at the possibility of the third party doctrine coming into play in a later CSAM-related Fourth Amendment case; however, that moment has not yet arisen. United States v. Ackerman, 831 F.3d 1292, 1308 (10th Cir. 2016).
110. Walter v. United States, 447 U.S. 649, 656–57 (1980).

conducts its own search, and the government then repeats the private search without exceeding its parameters, the government search does not implicate the Fourth Amendment.[111] This doctrine was first glimpsed in *Coolidge,* and its contours were refined in two subsequent cases.[112] *Walter v. United States*[113] occupies one end of the spectrum of the private search doctrine, with *United States v. Jacobsen*[114] occupying the other end.[115]

In *Walter*, private actors handed unwatched film reels to government agents, describing them as contraband.[116] The Court held that when government agents watched the films without obtaining a search warrant, they performed an unconstitutional search under the Fourth Amendment because the government exceeded the scope of the private search that preceded it.[117] Had the private actors first watched the films before handing them over, the government presumably would not have violated the private search doctrine.[118]

In contrast, the Court held in *Jacobsen* that the government did not perform a "search" under the Fourth Amendment because it did not exceed the scope of the private search that preceded it.[119] *Jacobsen* involved federal agents opening a package previously opened by FedEx employees and testing the contents for cocaine.[120] The *Jacobsen* Court reasoned that the federal agents' invasions of the defendant's privacy must be tested by the extent to which they exceeded the scope of the FedEx employees' search.[121] FedEx employees frustrated the defendant's expectation of privacy by opening a damaged package and reporting its contents to the government, and federal agents learned nothing more than what the private search had discovered.[122]

---

111. *Id.*

112. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487–90 (1971); *Walter*, 447 U.S. at 656–57; United States v. Jacobsen, 466 U.S. 109, 114–15 (1984).

113. 447 U.S. 649 (1980).

114. 466 U.S. 109 (1984).

115. *Walter* found the government's conduct unconstitutional while *Jacobsen* reached the opposite conclusion. *Walter*, 447 U.S. at 656–57; *Jacobsen*, 466 U.S. at 115.

116. *Walter*, 447 U.S. at 651.

117. *Id.* at 657.

118. *See id.* at 657–58.

119. *Jacobsen*, 466 U.S. at 115–16.

120. *Id.* at 111–12.

121. *Id.* at 115–16.

122. *Id.* at 120.

a. Other Relevant Cases to the Private Search Doctrine

Subjecting luggage to a sniff test by a trained narcotics dog is not a search under the Fourth Amendment because the search can only reveal the existence of contraband, not any form of private information.[123] Thus, binary searches that can only reveal the existence of contraband are acceptable under the Fourth Amendment.[124] In allowing for such "binary searches," the Supreme Court further limited the extent of Fourth Amendment protections.

In contrast to the binary search decision, the Supreme Court restricted the reach of the private search doctrine when it held that merely because the government does not compel a private search does not prove that the search in question is private.[125] When a private railroad company mandated breath and urine tests for its employees in response to regulations issued by a federal agency, the Court held those tests were searches under the Fourth Amendment.[126] In this sense, private actors may be unlawfully deputized by the government even without direct orders in situations where they are sufficiently nudged into performing the government's desired search.[127]

3. CSAM-Related Fourth Amendment Cases

United States v. Ackerman,[128] a Tenth Circuit decision authored by future Supreme Court Justice GORSUCH, set limits on the private search doctrine by ruling against the anti-CSAM union of government, NCMEC, and technology companies.[129] *Ackerman* held that NCMEC was a government entity for Fourth Amendment purposes because it was statutorily obliged to act as a national clearinghouse for CSAM reports, and in this role, its search of a defendant's email was unlawful because it did not seek a warrant.[130] NCMEC's search was unlawful because it either (1) conducted an impermissible warrantless search as a government entity or, (2) acting as the govern-

123. United States v. Place, 462 U.S. 696, 707 (1983).

124. *Id.*

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

126. *Id.* at 614.

127. *See id.* at 615–16. The Court did find that the tests were reasonable searches under the Fourth Amendment, but the Court's acknowledgement that the Fourth Amendment was implicated implies that there must be a situation in which such a search would be unreasonable. *See id.*

128. 831 F.3d 1292 (10th Cir. 2016).

129. *Id.* at 1295.

130. *Id.* at 1296.

ment's agent, exceeded the scope of the internet service provider (ISP)'s search that preceded it.[131]

NCMEC exceeded the search of the ISP before it because the ISP identified suspect images using only its hashing algorithm and forwarded the images to NCMEC without inspecting them.[132] Once NCMEC received the images, its agents inspected the images and identified them as CSAM.[133] Thus, NCMEC's search exceeded the scope of the search that preceded it because the images were not previously inspected.[134]

The First Circuit applied *Ackerman* to reach a different conclusion in *United States v. Powell*[135] when it held that NCMEC's warrantless viewing of screenshots taken by a chat website was lawful because NCMEC did not exceed the scope of the chat website's search.[136] The chat website, Omegle, opened and viewed the suspect screenshots before forwarding them to NCMEC.[137] In so doing, NCMEC could not violate the private search doctrine because its viewing of the defendant's screenshots simply repeated the same search Omegle performed.[138]

The Fifth Circuit strengthened the government's search power in *United States v. Reddick*[139] when it held that the critical inquiry under the Fourth Amendment is whether authorities obtained information to which the defendant's expectation of privacy had not already been frustrated.[140] The court further held that police did not violate a defendant's Fourth Amendment rights by reviewing images the defendant uploaded to a cloud hosting service because the defendant's expectation of privacy was frustrated by the private search.[141] The Fifth Circuit's approach thus obviates the need for the ISP to conduct its own inspection of the suspect images to satisfy the private search doctrine.[142] Instead, simply by running a hash algorithm to identify suspect images and forwarding those images

131. *Id.* at 1295–99, 1300–03.
132. *Id.* at 1305–06.
133. *Id.*
134. *Id.*
135. 925 F.3d 1 (1st Cir. 2018).
136. *Id.* at 6.
137. *Id.* at 3–4.
138. *Id.*
139. 900 F.3d 636 (5th Cir. 2018).
140. *Id.* at 638.
141. *Id.* at 639.
142. *Reddick*'s interpretation of the private search doctrine is more expansive than the Tenth and First Circuits because the Fifth Circuit held that hash value matching is so precise that there was no need for the ISP agent to personally inspect the files prior to sending them to law enforcement. *See id.* In this way, *Reddick* may be seen as expanding the reach of *Jacobsen*, where agents repeated a

to law enforcement, the technology company has already frustrated the image owner's expectation of privacy, and any further searches by law enforcement are valid.[143]

Despite appearing to veer from the Tenth Circuit's interpretation of the private search doctrine, the Fifth Circuit still tried to keep its holding in line with *Ackerman*.[144] The majority in *Reddick* reasoned that their conclusion was distinguishable from *Ackerman* because, in *Ackerman*, the detective opened email attachments that had never been previously inspected (either by the algorithm or a human agent), whereas, in *Reddick*, the detective only opened files previously inspected by the algorithm.[145]

The Sixth Circuit followed the First and Fifth Circuits in holding against a defendant in a Fourth Amendment CSAM-related case.[146] *United States v. Miller*[147] held that a defendant's claim that a police detective violated the private search doctrine failed because when there is a "virtual certainty" that the government's search will disclose nothing more than what a private party's earlier search has revealed, no Fourth Amendment search occurs.[148] The *Miller* court reasoned that Google's hash-value algorithm's "near-perfect accuracy" meant that the detective's search was unlikely to sweep up any private information beyond what Google had already identified and inspected.[149]

The Seventh Circuit created a new opening for technology companies seeking to restrict CSAM on their platforms in *United States v. Bebris*.[150] In *Bebris*, the court held that Facebook did not act as a government agent when it reviewed messages on its servers for CSAM and then reported that information to NCMEC.[151] In addition, the court described an "independent business purpose" as an acceptable justification for a technology company to move to eradicate CSAM on its platform.[152] When a company acts with "independent business purpose" and its actions comport with govern-

---

physical search by private actors and did not merely rely on the private actors' report. *See* United States v. Jacobsen, 466 U.S. 109, 118–19 (1984).

143. *See Reddick*, 900 F.3d at 639.

144. *See id.* at 639–40.

145. *Id.*

146. United States v. Miller, 982 F.3d 412, 418 (6th Cir. 2020).

147. 982 F.3d 412 (6th Cir. 2020).

148. *Id.* at 417–18.

149. *Id.* at 418.

150. *See* United States v. Bebris, 4 F.4th 551, 561–62 (7th Cir. 2021). The "new opening" refers to the Court's discussion of a technology company's "independent business purpose." *See id.*

151. *Id.*

152. *Id.*

ment intentions, the company merely acts with mutual purpose and not out of compulsion.[153] Under these circumstances, a company's actions do not implicate the private search doctrine or the Fourth Amendment.[154]

Finally, the Ninth Circuit interrupted the trend of pro-government decisions when it held in *United States v. Wilson*[155] that the government's actions exceeded the limits of the private search doctrine.[156] In *Wilson*, the court held that the government learned new, critical information not revealed by a previous private search when it viewed attachments that no Google employee had previously viewed.[157] In addition, Google's algorithm merely labeled the images "A1" and provided no description before sending them to the government.[158] Therefore, when the government opened the images, it was not accessing information consistent with Google's report, rather it was accessing new information.[159] Lastly, even if Google employees had viewed the images used by its algorithm, the defendant's expectation of privacy in his own images would not have been frustrated.[160] The defendant's expectation of privacy would not have been frustrated by Google's search because Google employees did not view his images, but instead viewed other images identified as CSAM.[161] Google's hash-value algorithm then reported the defendant's images as exact copies of the previously identified CSAM images.[162] Thus, no inspection of the *defendant's* images took place, and his expectation of privacy was not frustrated.[163]

In reaching its decision, the *Wilson* court emphasized the personal nature of Fourth Amendment rights.[164] The court likened Google and the government's actions to one in which the police search a person's house and discover contraband along with a note specifying that another person has exact copies of that contra-

153. *Id.*
154. *Id.*
155. 13 F.4th 961 (9th Cir. 2021).
156. *Id.* at 974–75.
157. *Id.* at 974.
158. *Id.* (describing the "A1" designation as resulting from Google's proprietary technology and providing no further description of what the "A1" designation meant).
159. *Id.*
160. *Wilson,* 13 F.4th at 974–75.
161. *Id.* at 975.
162. *Id.*
163. *Id.*
164. *Id.*

band.[165] Without a warrant, the police may not use that note as a pretext to then search the other person's house and seize the contraband.[166]

The Ninth Circuit described a "growing tension in the circuits" surrounding application of the private search doctrine in CSAM cases.[167] The *Wilson* court found common cause with the *Ackerman* court, finding the Tenth Circuit's analysis "consistent" with the Ninth Circuit's.[168] However, the Fifth and Sixth Circuits, in *Reddick* and *Miller*, reached different conclusions.[169]

The Ninth Circuit's decision was consistent with private search doctrine cases not related to hash value matching, such as the Sixth Circuit's *United States v. Lichtenberger*,[170] a case in which a defendant's girlfriend showed police a computer she said contained CSAM.[171] The girlfriend, however, could not remember if the pictures she showed to the police were the same as the ones she had viewed earlier.[172] Therefore, the Sixth Circuit held that the scope of the government search exceeded that of the private search that preceded it.[173] Similarly, in the Eleventh Circuit case of *United States v. Sparks*,[174] a store employee and her fiancé discovered a phone containing CSAM and showed the phone to police.[175] The police officer then viewed two videos containing CSAM, but the private parties had not viewed one of the videos.[176] Thus, the Eleventh Circuit held that the government's search was barred by the private search doctrine because the scope of the government search exceeded the private search that preceded it.[177]

4. Carpenter v. United States

The Supreme Court's most recent opinion addressing the intersection of technology and the Fourth Amendment came in 2018,

165. *Wilson*, 13 F.4th at 975.
166. *Id.*
167. *Id.* at 976.
168. *Id.* at 977.
169. *Id.* at 978.
170. 786 F.3d 478 (6th Cir. 2015).
171. *Wilson*, 13 F.4th at 977; United States v. Lichtenberger, 786 F.3d 478, 480 (6th Cir. 2015).
172. *Lichtenberger*, 768 F.3d at 481.
173. *Id.* at 485.
174. 806 F.3d 1323 (11th Cir. 2015).
175. *Id.* at 1329 (overruled on other grounds by United States v. Ross, 963 F.3d 1056 (11th Cir. 2020)).
176. *Id.* at 1335.
177. *Id.*

when *Carpenter v. United States*[178] addressed government searches in the context of cell phone data.[179] *Carpenter* held that a defendant's cell-site location information ("CSLI"), the information that results when a cell phone pings a cell tower, is protected by the Fourth Amendment.[180] Unlike its earlier ruling in *Miller,* when the Court approved of a bank providing a defendant's records to the government, the Court did not approve of a cell phone company releasing its records to the government because it was concerned with the "inescapable and automatic," as well as "deeply revealing" nature of the CSLI.[181] The Court also held that generally, police must obtain a warrant before searching a person's phone because modern phones contain an "immense storage capacity."[182]

Carpenter represents the Supreme Court's desire to prevent further erosion of Fourth Amendment protections to technological development.[183] In addition, four Supreme Court justices filed dissents, indicating that Fourth Amendment interpretation has yet to reach a firm consensus on the Supreme Court.[184]

II. ANALYSIS

A. Apple's Move Is Constitutional

Despite the controversy Apple's announcement provoked and the well-intentioned criticism the company received, Apple's anti-CSAM hashing technology is carefully crafted to survive Fourth Amendment scrutiny.[185] Thus, a Fourth Amendment legal challenge to Apple's move will likely fail. Apple's move is constitutional because Apple: (1) has an independent business purpose to search its users' phones, (2) satisfies all private search doctrine concerns addressed by the Ninth and Tenth Circuits, and (3) aligns itself with the First, Fifth, and Sixth Circuits' holdings in favor of

178. 138 S. Ct. 2206 (2018).

179. *Id.* at 2208–09.

180. *Id.*

181. United States v. Miller, 425 U.S. 435, 440 (1976); *Carpenter*, 138 S. Ct. at 2222–23.

182. *Carpenter*, 138 S. Ct. at 2214.

183. *Id.* at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

184. *Id.* at 2223–35 (Kennedy, THOMAS, & ALITO, JJ., dissenting); *id.* at 2235–46 (THOMAS, J., dissenting); *id.* at 2246–61 (ALITO & THOMAS, JJ., dissenting); *id.* at 2261–72 (GORSUCH, J., dissenting).

185. *See* APPLE, *supra* note 10, at 4–6 (revealing that Apple's plan requires human review and protects user privacy).

technology companies.[186] Finally, any judicial rejection of Apple's move would violate public policy.[187]

1. Apple Is Not Acting as a Government Agent When It Scans Its Users' Devices Because It Has an Independent Business Purpose to Conduct the Search

To avoid implicating the Fourth Amendment, Apple should first establish that it is not a government agent because it is installing its anti-CSAM hashing algorithm for an independent business purpose and not out of government compulsion.[188] By establishing this "independent business purpose," Apple can then justify its intrusion into its users' devices.[189]

A company may establish an independent business purpose to regulate CSAM on its platform in several ways. First, it may point to the direct and indirect costs associated with CSAM activity on its platform.[190] These costs include the time the company must spend dealing with customer complaints and organized customer action for failure to deal with CSAM.[191] Companies may also face image and reputational harms when they fail to confront CSAM appropriately.[192]

Second, a company may show that no federal law requires it to search for CSAM on its platform.[193] Although service providers are required to report CSAM to NCMEC upon discovery, any action

186. *See id.*

187. *See* 34 U.S.C. § 11293(b) (providing for an annual grant of federal funds to NCMEC to operate reporting services for CSAM and other activities); *see also* 18 U.S.C. § 2258A (providing that service providers have a duty to report CSAM on their platforms to NCMEC). The public policy favoring public-private partnerships against CSAM may also be evidenced by 18 U.S.C. § 2258B, which provides immunity for providers and their officers for actions arising out of their reporting responsibilities under 18 U.S.C. § 2258A.

188. *See* United States v. Bebris, 4 F.4th 551, 561–62 (7th Cir. 2021) (discussing the importance of a private company's "independent business purpose" in establishing that the company did not act out of government coercion).

189. *See id.*

190. *See id.*

191. *See id.*; *see also* Brief for Facebook, Inc. as Amicus Curiae Supporting Appellee, United States v. Bebris, 4 F.4th 551 (2021) (No. 20-3291), 2021 WL 955054, at *10–11 (describing Facebook's decision to confront CSAM as one motivated by a desire to be a "good corporate citizen" and because the company believes child pornography "abhorrent").

192. *See Bebris*, 4 F.4th at 561; *see also* Brief for Facebook, Inc. as Amicus Curiae Supporting Appellee, United States v. Bebris, 4 F.4th 551 (2021) (No. 20-3291), 2021 WL 955054, at *10 (supporting statement that no business that valued its image and reputation would desire to be publicly associated with child sexual exploitation).

193. *See* 18 U.S.C. § 2258A (stating that service providers have a duty to report CSAM they discover on their platforms to NCMEC, but no duty to search);

taken to search for CSAM is based only on the discretion of the provider.[194]

Finally, a company may demonstrate that working toward a common purpose with government does not make the company into the government's agent.[195] Instead, public-private partnerships emerging out of a joint desire to improve society represent a public policy that courts should acknowledge.[196]

First, Apple is not acting as a government agent when it installs its hashing algorithm on Apple devices because it has an independent business purpose for doing so. Many critics have subjected Apple to criticism for its failure to confront CSAM on its platform.[197] The direct costs of this failure include the reputational damage Apple has suffered for becoming "the greatest platform for distributing child porn."[198] Reputational damage can damage a corporation's profits, its main reason for existence.[199]

Apple's failure to confront CSAM has also incurred indirect costs. Because Apple's smartphone market share is so large, the effect of Apple devices becoming a haven for CSAM can presumably have society-wide effects.[200] A society that permits child abuse on a vast scale is likely a less productive and efficient society.[201] Less productive and efficient societies will undoubtedly lack the human

---

see also United States v. Ringland, 966 F.3d 731, 736 (8th Cir. 2020) ("Section 2258A does not require ESPs to seek out and discover violations.").

194. *See Ringland*, 966 F.3d at 736.

195. *See* United States v. Koenig, 856 F.2d 843, 849 (7th Cir. 1988) (providing that "mere knowledge of another's independent action" does not constitute government acquiescence "absent some manifestation of consent and the ability to control").

196. The public policy favoring public-private partnerships against CSAM may also be evidenced by 18 U.S.C. § 2258B which provides immunity for providers and their officers for actions arising out of their reporting responsibilities under 18 U.S.C. § 2258A.

197. *See* Matt Burgess, *How Apple Can Fix Its Child Sexual Abuse Problem*, WIRED (Sept. 8, 2021, 6:00 AM), https://bit.ly/3pJdxyB [https://perma.cc/S9JV-28SG] (reporting that Apple faced an inquiry into child sexual abuse from the U.K. government and legislation from the European Commission mandating that technology companies scan for CSAM, and quoting a cybersecurity expert who described Apple's move as "long overdue").

198. Hollister, *supra* note 72.

199. *See, e.g.*, Michael Volkov, *Calculating the Incalculable: Reputational Damage*, VOLKOV L. BLOG (Aug. 30, 2015), https://bit.ly/3Gav87Z [https://perma.cc/JU3M-EDPL] (describing, for example, the reputational damage Subway suffered on discovery of spokesman Jared Fogle's acts of child sexual exploitation).

200. *See* STATISTA, *supra* note 54.

201. *See* CTR. FOR DISEASE CONTROL AND PREVENTION, COST OF CHILD ABUSE AND NEGLECT RIVAL OTHER MAJOR PUBLIC HEALTH PROBLEMS (2014), https://bit.ly/3rVXqOF [https://perma.cc/D7QG-9LNW] (reporting the financial cost of confirmed cases of child maltreatment as $124 billion per year).

capital necessary to sustain or increase demand for more Apple products and services.[202] Any CSAM permitted on Apple's devices negatively affects society as a whole, and in turn, Apple itself.

Second, Apple is not acting as a government agent because the government does not require Apple to search for CSAM on its platform.[203] Not only is there no law compelling Apple to act but the government has taken no overt steps to force Apple to act.[204] Instead, Apple is responding to private criticism and acting on its own concerns to clean up its platform.[205]

Finally, Apple is not acting as a government agent merely because the government shares a desire to combat CSAM.[206] When it searches its customers' devices without the government's prompting, Apple will act out of its own private business interest and not under government compulsion.[207]

2. *Apple's New Tools Satisfy All Private Search Doctrine Concerns Raised by the Ninth and Tenth Circuits*

Apple's new tools were carefully crafted to satisfy the private search doctrine concerns of the *Ackerman* court and the *Wilson* court.[208] *Ackerman* held that NCMEC exceeded the private search that preceded it because no human reviewed the selected images prior to NCMEC.[209] *Wilson* held that the private search doctrine was violated in three ways.[210] First, only an algorithm, and not a

202. *See id.* One may infer that child abuse on a society-wide level affects Apple's bottom line based on the previously cited cost of $124 billion per year and the fact that Apple depends largely on the health of the American economy to succeed. *See id.*; *see also* Lionel Sujay Vailshery, *Revenue of Apple by Geographical Region from the First Quarter of 2012 to 4th Quarter 2021*, STATISTA (Nov. 23, 2021), https://bit.ly/3o7fhAU [https://perma.cc/58SJ-NKCZ] (reporting that despite a growing international sales volume, the United States. still accounts for 40 percent of Apple's net sales).

203. *See* 18 U.S.C. § 2258A.

204. *See id.*; *see also* APPLE, *supra* note 10, at 6 (stating that, in the past, Apple has faced pressure from governments to degrade user privacy but has always resisted such demands).

205. *See* APPLE, *supra* note 10, at 6.

206. *See* United States v. Koenig, 856 F.2d 843, 849 (7th Cir. 1988) (providing that "mere knowledge of another's independent action" does not constitute government acquiescence "absent some manifestation of consent and the ability to control").

207. *See* United States v. Smith, 383 F.3d 700, 705 (8th Cir. 2004) (concluding that even with the government's knowledge and acquiescence to a private search, the private party still did not act under compulsion of government and the search did not implicate the Fourth Amendment).

208. *See* United States v. Ackerman, 831 F.3d 1292, 1292 (10th Cir. 2016); *see also* United States v. Wilson, 13 F.4th 961, 974–75 (9th Cir. 2021).

209. *See Ackerman*, 831 F.3d at 1305–06.

210. *Wilson*, 13 F.4th at 973–75.

human, reviewed the defendant's images at Google before they were sent to NCMEC.[211] Second, Google's process only allowed for employees to view stock CSAM images used by the algorithm, and not the suspect images used by defendant Wilson himself.[212] Third, the offending images were poorly marked by the algorithm and failed to provide an adequate explanation for the image's contents.[213]

Satisfying both *Ackerman* and the first point identified by *Wilson*, Apple will share no photo and no potentially incriminating information with NCMEC without human review.[214] Addressing *Wilson*'s second point, this human review will require an Apple employee to review the suspect images, and not merely the images used by the algorithm for matching purposes.[215] To meet *Wilson*'s third concern, Apple will fully describe the contents of the suspect photos to allow for proper verification by NCMEC employees.[216] By completing all these steps, Apple will fully satisfy the standard of the private search doctrine.[217] Those NCMEC or government employees who follow up on Apple's reports will be unable to expand the scope of the private search.[218] In addition, Apple will frustrate the defendant's expectation of privacy, meeting the standard identified by the *Wilson* court.[219]

3. *Apple's Move Aligns with First, Fifth, and Sixth Circuit Holdings Supporting Technology Companies Because Its Anti-CSAM Procedures Include Safeguards Beyond Those Used in These Cases*

The First Circuit in *Powell* held that NCMEC did not violate the private search doctrine because it repeated the exact search that the chat website Omegle conducted previously.[220] Likewise, Apple's technology and anti-CSAM investigation, including

211. *Id.* at 973–74.
212. *Id.* at 975.
213. *Id.* at 974.
214. APPLE, *supra* note 10, at 5.
215. *Id.*
216. *See id.* (detailing that Apple will only report images known as suspected CSAM because they exist in NCMEC's database of verified CSAM images).
217. *See* Walter v. United States, 447 U.S. 649, 656–57 (1980); *see also* United States v. Jacobsen, 466 U.S. 109, 115–17 (1984).
218. *See* APPLE, *supra* note 10, at 5–6. Assuming that Apple's procedures are followed correctly, there will be no opportunity for NCMEC to violate the private search doctrine because there will be no unexposed information left for NCMEC to expose. *See id.*
219. *See id.*; *see also Walter*, 447 U.S. at 656–57; United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018).
220. United States v. Powell, 925 F.3d 1, 6 (1st Cir. 2018).

mandatory human review of all suspect images, will not allow for a situation in which NCMEC might violate the private search doctrine.[221]

In *Reddick*, the Fifth Circuit held that a government agent inspecting suspect images did not violate the private search doctrine even though the private search was conducted only by algorithm.[222] Here, Apple's process goes beyond the Fifth Circuit's holding by ensuring that human review of all suspect images identified by the algorithm will occur prior to sending a report.[223]

In a similar holding to *Reddick*, the Sixth Circuit held in *Miller* that Google's hash-value algorithm was so close to perfect that human review was unnecessary.[224] Again, Apple exceeds this standard because not only is it using the best available hashing technology to find images, but it is also including human review once those images are identified.[225]

4. Any Judicial Rejection of Apple's Move Violates Public Policy

Given the strong public policy favoring the eradication of CSAM, any judicial rejection of Apple's move would violate public policy.[226] The U.S. Congress expressed this policy when it enacted statutes providing for federal funding of NCMEC and mandating the reporting of any CSAM providers discovered.[227] In addition, Congress has enacted numerous other statutes emphasizing a desire to protect victims of child sexual abuse and to punish those responsible for child sexual abuse and CSAM.[228] Executive Branch agen-

221. *See* APPLE, *supra* note 10, at 5–6 (assuming that Apple's protocol is followed).

222. *Reddick*, 900 F.3d at 639.

223. *See* APPLE, *supra* note 10, at 5–6.

224. United States v. Miller, 982 F.3d 412, 417–18 (6th Cir. 2020).

225. *See* APPLE, CSAM DETECTION: TECHNICAL SUMMARY 4 (2021), https://apple.co/31nFiU1 [https://perma.cc/WBM7-UBFV] (describing NeuralHash, Apple's hashing technology). There is only a one-in-one-trillion chance that Apple's hashing technology will identify an incorrect account. *Id.*

226. *Public Policy*, BLACK'S LAW DICTIONARY (11th ed. 2019). "Public policy" is the collective rules, principles, or approaches to problems that affect the commonwealth or (esp.) promote the general good; specif., principles and standards regarded by the legislature or by the courts as being of fundamental concern to the state and the whole of society. *Id.*

227. *See* 34 U.S.C. § 11293(b); *see also* 18 U.S.C. § 2258A.

228. *See generally* 18 U.S.C. § 2259B (providing a reserve fund for victims of child pornography); *see also* 18 U.S.C. § 2252 (providing criminal penalties for production or possession of CSAM); 18 U.S.C. § 2259 (providing for mandatory restitution to victims of CSAM trafficking).

cies have also expressed this anti-CSAM policy through several administrations.[229]

Apple's move strongly comports with the will of Congress because it will significantly reduce the production and transmission of CSAM.[230] Thus, any judicial act that disrupts Apple's move will violate public policy as expressed by the American people's elected representatives.

B. The Supreme Court Should Adopt a Synthesized Rule

To resolve the circuit split regarding CSAM-related Fourth Amendment cases, the Supreme Court should grant certiorari to a related case.[231] Then, the Court should adopt a rule that resolves the concerns identified by the Ninth and Tenth Circuits with the holdings of the First, Fifth, Sixth, and Seventh Circuits.[232] This rule would permit technology companies to use hashing to identify CSAM on their platforms and refer those responsible to law enforcement, but only with certain constitutional safeguards in place.

One such possible rule would be: Technology companies with an independent business purpose that search for CSAM on their platforms and forward the results of their findings to NCMEC or the government do not implicate the Fourth Amendment, provided that the search conducted by NCMEC or the government survives an analysis under the private search doctrine.[233] In addition, the following clarifying instruction should be included: NCMEC is not acting as a government agent when it conducts a search of suspected CSAM it received from a technology company, provided that

229. *See* U.S. DEP'T OF JUSTICE, *supra* note 21; *see also* U.S. SENT'G COMM'N, *supra* note 24; *FBI Budget Request for Fiscal Year 2020: Hearing Before the Subcomm. on Com., Just., Sci. & Related Agencies of the H. Appropriations Comm.*, 116th Cong. (2019) (statement of Christopher Wray, Director, Federal Bureau of Investigation), https://bit.ly/3pwKbUV [https://perma.cc/QXZ9-3WNA].

230. Because Apple controls such a large share of the smartphone market and because it has failed to report significant CSAM, it may be inferred that, when implemented, Apple's initiative will significantly reduce the quantity of available CSAM. *See* NCMEC REPORTS, *supra* note 41; *see also* STATISTA, SUBSCRIBER SHARE HELD BY SMARTPHONE OPERATING SYSTEMS IN THE UNITED STATES FROM 2012 TO 2021 (2021), https://bit.ly/3ptpR6L [https://perma.cc/4WC2-Y78R].

231. *See* United States v. Wilson, 13 F.4th 961, 976 (9th Cir. 2021) (describing a "growing tension in the circuits" over CSAM-related Fourth Amendment interpretation); *see also* Sup. Ct. Rule 10(a) (specifying that one of the standards for the Supreme Court to grant certiorari is when U.S. courts of appeals are in conflict on the same "important matter").

232. *See Wilson*, 13 F.4th at 976–78 (summarizing the differences between the U.S. courts of appeals on this Comment's topic).

233. *See* United States v. Bebris, 4 F.4th 551, 561–62 (7th Cir. 2021) (discussing the importance of a private company's "independent business purpose" in establishing that the company did not act out of government coercion).

NCMEC does not violate the private search doctrine.[234] Finally, the Court should acknowledge the public policy that supports the eradication of CSAM: Public policy strongly favors techniques, procedures, and technologies that seek to eradicate or disrupt the production and dissemination of CSAM.[235]

The advantage of such a rule is that it would offer clarity to the circuit courts as they apply established Fourth Amendment jurisprudence to modern, technology-related legal problems. Requiring technology companies to act with an independent business purpose would protect defendants who can show that the technology company acted out of government coercion.[236] In addition, it is important to clarify NCMEC's role in the process.[237] The Supreme Court should recognize NCMEC's important, congressionally supported, role in bringing to justice those who violate CSAM laws.[238] The Court may do so while still respecting criminal defendants' Fourth Amendment rights by simply requiring that all actors abide by the private search doctrine.[239] Finally, the Court's acknowledgement of the public policy against CSAM will indicate to lower courts that any legal analysis of CSAM cases must recognize the importance of this public policy.

---

234. *See* United States v. Ackerman, 831 F.3d 1292, 1296 (10th Cir. 2016) (addressing the Tenth Circuit's holding that NCMEC was acting as a governmental entity).

235. *See generally* 18 U.S.C. § 2259B (providing a reserve fund for victims of child pornography); *see also* 18 U.S.C. § 2252 (providing criminal penalties for production or possession of CSAM); 18 U.S.C. § 2259 (providing for mandatory restitution to victims of CSAM trafficking); 34 U.S.C. § 11293(b); 18 U.S.C. § 2258A.

236. Admittedly, it may be difficult for a criminal defendant to credibly argue that a large technology company such as Apple does *not* have an independent business purpose in eradicating CSAM on its platform. *See* Brief for Facebook, Inc. as Amicus Curiae Supporting Appellee, United States v. Bebris, 4 F.4th 551 (2021) (No. 20-3291), 2021 WL 955054, at *10 (supporting statement that no business that valued its image and reputation would desire to be publicly associated with child sexual exploitation). The public desire for companies to combat CSAM and the reputational damage a company may suffer from allowing their platforms to be infested with CSAM provides a strong basis for private, independent anti-CSAM action. *Id.* However, this rule would still provide a defense for criminal defendants should the government become overly involved in prompting private action. *See* Walter v. United States, 447 U.S. 649, 656–57 (1980) (holding the government's search unconstitutional as violating the private search doctrine).

237. *See* United States v. Ackerman, 831 F.3d 1292, 1296 (10th Cir. 2016) (addressing the Tenth Circuit's holding that NCMEC was acting as a governmental entity).

238. *See* 34 U.S.C. § 11293(b); *see also* 18 U.S.C. § 2258A.

239. *See* Walter v. United States, 447 U.S. 649, 656–57 (1980) (holding the government's search unconstitutional as violating the private search doctrine).

CONCLUSION

> Whoever receives one such child in my name receives me, but whoever causes one of these little ones who believe in me to sin, it would be better for him to have a great millstone fastened around his neck and to be drowned in the depth of the sea.[240]

A society that does not protect its children will not long endure. The U.S. legal system must find an accommodation between the need to protect children from horrific abuse and the need to protect citizens' constitutional rights. With an appropriately structured legal rule, neither of these principles will be sacrificed.

Citizens will not suffer an erosion of their Fourth Amendment rights should courts continue to safeguard the private search doctrine in CSAM cases.[241] Similarly, children will be adequately protected should courts guarantee criminal defendants their rights against unreasonable search and seizure.[242]

Apple may scan its users' devices for CSAM without violating the Fourth Amendment.[243] Once Apple discovers CSAM, and after human review, Apple is then legally required to refer that information to NCMEC.[244] After NCMEC review, law enforcement may then charge individuals implicated in these CSAM reports from Apple.[245] Assuming that Apple, NCMEC, and law enforcement follow all procedures as planned and directed, criminal defendants are unlikely to succeed in a Fourth Amendment legal challenge against Apple, NCMEC, or law enforcement.[246]

---

240. *Matthew* 18:2–6 (English Standard).

241. *See generally* SOLOVE & SCHWARTZ, *supra* note 81 (discussing at length the development of Fourth Amendment jurisprudence and the protections of the private search doctrine).

242. *See* Joseph Zabel, *Public Surveillance Through Private Eyes: The Case of the Earn It Act and the Fourth Amendment*, 2020 U. ILL. L. REV. ONLINE 167, 173 (2020) (describing how, in drafting the Earn It Act, legislators walk a fine line between the government's deputizing tech companies and failing to provide any meaningful incentives to influence tech companies to disrupt CSAM).

243. *See* APPLE, *supra* note 10, at 5–6 (assuming Apple's procedures are followed).

244. *See* 18 U.S.C. § 2258A.

245. *See* 18 U.S.C. § 2251; *see also* 18 U.S.C. § 2252.

246. *See* APPLE, *supra* note 10, at 5–6.