SCANNING THE CLOUD: WHAT WILL APPLE REALLY KEEP PRIVATE?

Alexa Sullivan*

I. Introduction

Apple, a tech giant that has historically boasted its ability to prioritize user privacy, has proposed new scanning technology to be installed on user’s personal devices for the purpose of detecting Child Sexual Abuse Material (“CSAM”), suggesting that its loyalty to consumers may have its limits.¹ The online distribution of sexual abuse images of children, predating the era of advanced digital technology, has been a continuously growing problem for law enforcement agencies across the United States.²

¹ See Expanding Protections for Children, APPLE INC. (Sept. 3, 2021), archived at https://perma.cc/4XXV-92T9 (describing newly proposed child safety features “to help limit the spread of Child Sexual Abuse Material.”). According to Apple, this will allow the company to detect and report CSAM images stored in iCloud to the National Center for Missing and Exploited children (NCMEC), working “in collaboration with law enforcement agencies across the United States.” Id. See also Joseph Menn & Julia Love, Exclusive: Apple’s child protection features spark concern within its own ranks -sources, REUTERS (Aug. 12, 2021), archived at https://perma.cc/LQY5-BLDT (commenting that some Apple employees are openly opposed to the new features, “a notable turn in a company famed for its secretive culture”); How Big Tech is Finally Tackling Cybersecurity, CB INSIGHTS (Mar. 27, 2019), archived at https://perma.cc/AXN6-A8T9 (describing Apple and other tech companies’ cybersecurity practices to protect user data). “Apple has always prided itself with being deeply focused on user privacy and hasn’t come under the scrutiny of other FAMGA companies.” Id. See also Adi Roberston, Apple’s controversial new child protection features, explained, THE VERGE (Aug 10, 2021), archived at https://perma.cc/3BV5-TX9Q (contrasting Apple’s reputation for protecting user privacy with newly proposed child protection features). “Apple has used on-device processing to bolster its privacy credentials in the past.” Id.
enforcement. As a result of technology rapidly advancing, it is far easier for people to possess and share illicit materials over the internet, as well as through personal devices such as smartphones and laptops.

To counteract this issue, the government has encouraged big tech companies to aid in preventing the spread of child sex abuse materials by taking a more proactive role in regulating their platforms. Specifically, the government is considering passing the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020 (“EARN IT”), which is intended to coerce tech companies to aggressively police for child sex abuse images on their services. In response to this initiative, Apple’s proposed on-device scanning program will also include a “reporting system that sends data to the

---

2 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), archived at https://perma.cc/4RQ4-M5SR [hereinafter The Internet is Overrun] (commenting on the increasing online presence and sharing of child sex abuse images). “Reports to the authorities typically contain more than one image, and last year encompassed the record 45 million photos and videos, according to the National Center for Missing and Exploited Children.” Id.

3 See id. (commenting on the increasing spread of child pornography due to smartphones, social media, and other platforms); Olivia Solon, Child sexual abuse images and online exploitation surge during pandemic, NBC NEWS (Apr. 23, 2020), archived at https://perma.cc/F7MD-QCC4 (noting how the COVID-19 pandemic has increased people’s online use, leading to an increase in demand for illicit child content). See also Slater Teague, Sullivan County man arrested on child porn charges, WJHL (Aug. 30, 2021), archived at https://perma.cc/5Z56-4U6V (describing man being arrested after authorities were informed of images of child pornography sent on Snapchat); Schoharie County man sentenced to 12 years over child pornography, WTEN (Aug. 14, 2021), archived at https://perma.cc/26Z5-QD2C (highlighting arrested man who “download[ed] more than 13,000 still images and 2,400 videos from the internet.”).

4 See Kevin Reed, Apple to work with law enforcement to scan personal photo libraries for child abuse content, WORLD SOCIALIST WEB SITE (Aug. 11, 2021), archived at https://perma.cc/DU6S-HVTH (noting Apple’s collaboration with NCMEC and law enforcement to stop the spread of child pornography).

5 See Hannah Quay-de la Vallee & Mana Azarmi, The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions, CTR. FOR DEMOCRACY & TECH. (Aug. 25, 2020), archived at https://perma.cc/L6MU-C5HF (analyzing the EARN IT Act and its implications on privacy rights). “EARN IT seeks to deal with the scourge of online child exploitation by coercing service providers to more aggressively police such content on their platforms.” Id.
National Center for Missing and Exploited Children (NCMEC). . .”

Apple still attempts to protect user privacy concerns by providing more transparency to the system’s device encryption functionality.

II. History

A. The Fourth Amendment

An individual citizen’s right to privacy is largely derived from the Fourth Amendment. Under this amendment, an individual can assert their right against governmental intrusion if they have an actual, subjective expectation of privacy that society finds reasonable. The

6 See Our Work, NAT’L CTR. FOR MISSING & EXPLOITED CHILD. (2021), archived at https://perma.cc/D6HX-8CYK (outlining the purpose of NCMEC and the active assistance it gives to law enforcement and others). “NCMEC proactively provides assistance to victims, families, law enforcement, social service agencies, mental health agencies and others when they need help with a missing, exploited, or recovered child.” Id. See also Reed, supra note 4 (describing Apple’s role in assisting law enforcement with their initiative to stop the spread of CSAM).

7 See Matthew Panzarino, Interview: Apple’s head of Privacy details child abuse detection and Messages safety features, TECH CRUNCH (Aug. 10, 2021), archived at https://perma.cc/9QSU-5UVS (detailing child abuse detection safety features to address consumer concerns). In an interview with Erik Neuenschwander, the head of Privacy at Apple, he begins to explain the features Apple is implementing in detail, such as “It seems clear from Apple’s willingness to provide access and its ongoing FAQ’s and press briefings [. . .] that it feels that it has a good solution here.” Id.

8 See U.S. CONST. amend. IV (defining the scope of an individual’s right to privacy). The Fourth Amendment reads, “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Id. See e.g., Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that under the Fourteenth Amendment the states must comply with the provisions of the Fourth Amendment); Oliver v. U.S., 466 U.S. 170, 178 (1984) (holding that “a search proscribed by the [Fourth] Amendment” occurs when certain government intrusions “violate reasonable expectations of privacy”); Terry v. Ohio, 392 U.S. 1, 9 (1968) (noting “wherever an individual may harbor a reasonable ‘expectation of privacy,’ he is entitled to be free from unreasonable government intrusion”). See also U.S. CONST. amend. XIV, § 1 (extending the Fourth Amendment guarantee against unlawful searches and seizures to the states).

9 See Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (recognizing that there is a two-part test for determining privacy rights). The Fourth Amendment’s prohibition on unreasonable searches only applies when a person has “exhibited an actual (subjective) expectation of privacy . . . that society is prepared
court has held that a citizen maintains a reasonable right to privacy protections in the context of telephone conversations, location data, inside one’s home, and closed containers. Nevertheless, these protections are not absolute, as a person will not have a reasonable expectation of privacy when exposing their matters to the world. Therefore, the right to privacy therefore may be waived if a person’s actions no longer demonstrate a reasonable expectation of privacy, even if unintentional.

Government agents must conduct a “search or seizure” of a citizen for the Fourth Amendment to apply, which generally requires probable cause.

A search has been defined as a governmental
to recognize as ‘reasonable.’” Id. See also Smith v. Maryland, 442 U.S. 735, 740 (1979) (holding that protection under Fourth Amendment “depends on whether the person invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’”).

See Katz, 389 U.S. 347 at 352 (suggesting a person using a telephone “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.”). After entering and paying the toll, the phone booth became a “temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.” Id. at 361. See also Carpenter v. U.S., 138 S. Ct. 2206, 2220 (2018) (holding that citizens retain a Fourth Amendment right in their cell phone location data). See also Florida v. Jardines, 569 U.S. 1, 6 (2013) (stating that “when it comes to the Fourth Amendment, the home is first among equals.”); Payton v. New York, 445 U.S. 573, 589–90 (1980) (clarifying that the Fourth Amendment undeniably protects an individual’s zone of privacy while physical in one’s home); Silverman v. U.S., 365 U.S. 505, 511 (1961) (holding that homeowners have a reasonable expectation of privacy). “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.” Id. See David A. Couillard, Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2211 (2009) (discussing that one maintains a privacy interest in a closed container belonging to them despite the relinquishment of control or public placement).

See Katz, 389 U.S. 347 at 361 (Harlan, J., concurring) (explaining that privacy rights are determined based on reasonable expectations). “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” Id. at 351. In other instances, “what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” Id.

See id. (analyzing circumstances when an individual exposes private matters to third parties and the public resulting in diminished privacy expectations).

See Overview of the Fourth Amendment, 35 GEO. L. J. ANN. REV. CRIM. PROC. 3, 3–4 (2006) (indicating that probable cause is required for most governmental intrusions on privacy interests referenced by the Fourth Amendment).
intrusion of private property in order to obtain information that infringes upon a person's legitimate expectation of privacy. Despite this general presumption, there are some circumstantial exceptions allowing the government to avoid the probable cause requirement. Specifically, the court has recognized the exception of consent, where an individual, or a third party sharing common authority, expressly or implicitly consents to the warrantless search based on their prior actions or agreements. Further, third party consent may be valid even if the consent was given in the defendant's absence by a woman who also lived there; Frazier v. Cupp, 394 U.S. 731, 740 (1969) (holding the joint user of duffel bag had authority to consent to a search of the bag);
without mutual use of the property if the consenting party has control of the property as the express or implied agent of the owner.\textsuperscript{17} It is clear from precedential case law that any “warrant” issued for mass surveillance absent suspicion would be an unconstitutional, general warrant.\textsuperscript{18}

\textsuperscript{17} See U.S. v. Matlock, 415 U.S. 164, 171 (1974) (explaining the test for third party binding consent). The test for third party consent is satisfied when “common authority”, or shared access that gives the third-party independent control exists, and there is an objective assumption by the “first party” of the risk of disclosure by the third-party. \textit{Id.} See also U.S. v. Bennett, 709 F.2d 803, 806 (2d Cir. 1983) (holding a government informant is able to consent if the court determines a private searcher had permission to enter location). See also, e.g., U.S. v. Alexander, 573 F.3d 465, 474 (7th Cir. 2009) (holding that an agent of a repossession may give valid consent to search a vehicle to be repossessed); U.S. v. Baswell, 792 F.2d 755, 759 (8th Cir. 1986) (holding a custodian with only limited access to property may give valid consent to search under agency theory).

\textsuperscript{18} See U.S. v. Bridges, 344 F. 3d 1010, 1017–18 (9th Cir. 2003) (finding warrant issued to be unconstitutional because the language describing the items to be seized by law enforcement was too broad with no definitive scope); Stanford v. St. of Tex., 379 U.S. 476, 481 (1965) (stating that the Fourth Amendment “reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever ‘be secure in their persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant”); Boyd v. U.S., 116 U.S. 616, 630–31, (1886) (holding that the Fourth Amendment requires search warrants to state with reasonable particularity what items are being targeted for search or, alternatively, what criminal activity is suspected of having been perpetrated).
1. The Expanded Scope of the Fourth Amendment for State Action

The Fourth Amendment acts as a restriction on the government, and does not apply to the actions of private parties. As such, private actors are permitted to access user data with significantly less restrictions than governmental entities. If a private party, like a tech company, voluntarily submits user data information to the Government, the Fourth Amendment is generally not implicated. The Supreme Court has held that a person cannot have a legitimate expectation of privacy if the information is voluntarily given to a third party. The Third-Party Doctrine, otherwise known as the Stranger Principle, allows for an individual’s information to be retrieved from third parties based on the presumption that there is no longer a

---

19 See U.S. v. Jacobsen, 466 U.S. 109, 130 (1984) (concluding that the Fourth Amendment is not generally applicable to searches and seizures performed by private entities). The court has held the Fourth Amendment is not implicated in a search or seizure effected by a private individual who is not acting on behalf of the Government or with the participation or knowledge of any governmental official[],” even if the search is an unreasonable one. Id.

20 See U.S. Const. amend. XIV, § 1 (establishing sovereignty of citizens and private conduct). See also Equal Protection of The Laws, JUSTIA (2021), archived at https://perma.cc/UK89-GPKL (explaining that the first section of the Fourteenth Amendment “erects no shield against merely private conduct, however discriminatory or wrongful.”). “The Fourteenth Amendment, by its terms, limits discrimination only by governmental entities, not by private parties.” Id.

21 See Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that there can be no expectation of privacy when the information is given to a third party). See also U.S. v. Miller, 425 U.S. 435, 443 (1976) (noting the limitations of the Fourth Amendment under the Third-Party Doctrine). “[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” Id.

22 See Andrew William Bagley, Don’t Be Evil: The Fourth amendment in the Age of Google, National Security, and Digital Papers and Effects, 21 ALB. L.J. SCI. & TECH. 153, 173 (2011) (noting the Supreme Court decisions that held there cannot be a reasonable expectation of privacy for information disclosed to third parties). See also Smith, 442 U.S. at 745–46 (holding the installation of a pen register at the telephone company used to learn the telephone numbers called from a private telephone was not a search because the numbers called were to a third party phone company and therefore were not private); U.S. v. White, 401 U.S. 745, 752 (1971) (holding that a plaintiff assumes the risk of an invasion of privacy when information is dispensed to a third party).
reasonable expectation of privacy once the information has been disseminated.\textsuperscript{23} When someone maintains personal property on a third party's premises, that person still holds an expectation of privacy in it if the property is secured against others' access and the third party's right of access to the premises is limited.\textsuperscript{24} As the digital age has evolved, the Court has narrowed the application of the Third-Party Doctrine in limited circumstances when significant privacy concerns are implicated, such as cell phone location data.\textsuperscript{25}

However, there are generally two situations where it has been found that a private party may qualify as a government agent.\textsuperscript{26} First,

\textsuperscript{23} See Lon A. Berk, \textit{AFTER JONES, THE DELUGE: THE FOURTH AMENDMENT'S TREATMENT OF INFORMATION, BIG DATA AND THE CLOUD}, 14 J. High Tech. L. 1, 3 (2014) (analyzing the concept of the Stranger Principle under the Fourth Amendment). The Stranger Principle states the idea that there is no longer a legitimate privacy interest available to protect against search and seizures of that information if “a person gives control over [that] information to a third party.” \textit{Id.} \textit{See also} Katz v. U.S., 389 U.S. 347, 360–61 (1967) (Harlan, J. concurring) (providing that the core reason data is afforded Fourth Amendment protection is due to the reasonable expectations of privacy held by individuals).

\textsuperscript{24} See Stoner v. California, 376 U.S. 483, 489 (1964) (holding that a warrantless search of hotel room violated Fourth Amendment, even though one who purchases a hotel room gives implied permission to hotel personnel to enter to perform their duties); Chapman v. U.S., 365 U.S. 610, 616–18 (1961) (holding a search of house occupied by tenant violated Fourth Amendment, even though landlord had authority to enter house for some purposes); U.S. v. Johns, 851 F.2d 1131, 1133–36 (9th Cir. 1988) (implicitly recognizing reasonable expectation of privacy in rented storage unit); U.S. v. Rahme, 813 F.2d 31, 34 (2d Cir. 1987) (concluding where hotel guest failed to pay rent and rental period expired, hotel could lawfully take possession of items in room and guest had no reasonable expectation of privacy).

\textsuperscript{25} See Carpenter v. U.S., 138 S. Ct. 2206, 2219 (2018) (asserting that the Third-Party Doctrine is not absolute). The Fourth Amendment is not completely abandoned even when there are “diminished privacy interests” when information is knowingly shared with a third party. \textit{Id.} The analysis depends on “the nature of the particular documents sought” to determine whether “there is a legitimate ‘expectation of privacy’ concerning their contents.” \textit{Id.} (quoting U.S. v. Miller, 425 U.S. 435, 442 (1976)). \textit{See also} Kara Goldman et al., \textit{Privacy in the Digital Age}, AM. THINKER (July 19, 2013), archived at \url{www.perma.cc/0DkGzfhSDB} (discussing the reality of stored information by third party providers).

if the private party is acting “as an instrument or agent of the Government”, then the conduct constitutes state action and the Fourth Amendment applies.\textsuperscript{27} The Fourth Amendment generally requires that the government to obtain a search warrant predicated on probable cause when compelling a private party to perform a search on its behalf.\textsuperscript{28} Second, a private entity may act as an agent of the government intentionally, unknowingly, or can be coerced into doing so.\textsuperscript{29} In \textit{Skinner v. Railway Labor Executives’ Association}, the Supreme Court held that a private corporation taking action based on merely permissive governmental regulations that were not mandatory

\textsuperscript{27}See Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (holding that a private party may be considered a government agent when acting in the interest of the government). A private search can turn into a governmental search only in instances where the government shows some exercise of power over the private entity, such that the private entity may be said to have acted “as an ‘instrument’ or agent of the state” rather than for its own, private purposes. \textit{Id. See also} U.S. v. Jones, 231 F.3d 508, 517 (9th Cir. 2000) (holding private person acts as an instrument or agent of the government if the government “authorizes, directs and supervises that person’s activities and is aware of those activities.”); U.S. v. Feffer, 831 F.2d 734, 739 (7th Cir. 1987) (explaining the government agency or instrumentality analysis). The two-part analysis to determine when a private party acts as a government agent 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.” \textit{Id. See also} Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass’n, 531 U.S. 288, 295 (2001) (holding that state action may be found only if there is such a “‘close nexus between the State and the challenged action’ that seemingly private behavior ‘may be fairly treated as that of the States itself.’”).

\textsuperscript{28}See George v. Edholm, 752 F.3d 1206, 1216 (9th Cir. 2014) (holding a private doctor acts as a state actor when searching patient’s rectum for cocaine per police inducement or encouragement); U.S. v. Ackerman, 831 F.3d 1292, 1302 (10th Cir. 2016) (non-profit organization is state actor when intentionally assisting law enforcement to find child pornography); U.S. v. Doe, 61 F.3d 107, 109 n.3 (1st Cir. 1995) (holding nongovernmental personnel manning airport security checkpoints are state actors when conducting searches for drugs due to FAA’s extensive administrative directives); Cassidy v. Chertoff, 471 F.3d 67, 74 (2d Cir. 2006) (concluding ferry operators are state actors when conducting legally-required searches of passenger automobiles and bags in accordance with Coast Guard-approved plan).

\textsuperscript{29}See \textit{Skinner}, 489 U.S. 602 at 615–16 (finding that railways act as government agents when they drug test employees pursuant to a government statute that strongly encourages such drug testing); Anirudh Krishna, \textit{Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse}, 109 CALIF. L. REV. 1581, 1610 (2021) (highlighting the leading case \textit{Skinner} where the government coerced private entities into acting on its behalf).
in nature could still be considered an agent of the government in the context of the Fourth Amendment. 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, the railway company Amtrak was found to be a government agent. Additionally, under the private search doctrine, the Fourth Amendment is implicated only if the government’s search expands the breadth and scope of a private party’s previous search. Conversely, if the scope of the search is not expanded and merely replicated, the government is not considered to have conducted a Fourth Amendment search.

---

30 See *Skinner*, 489 U.S. 602 at 615 (holding that the railways acted as government agents when implementing the FRA's two-pronged drug testing policy even though they were not compelled to do so); U.S. v. Stevenson, 727 F.3d 826, 829 (8th Cir. 2013) (expanding on situations where a private party’s search is still subject to the Fourth Amendment). “Even when a search is not required by law, however, if a statute or regulation so strongly encourages a private party to conduct a search that the search is not ‘primarily the result of private initiative,’ then the Fourth Amendment applies.” *Id.* See also Paul G. Reiter, *Admissibility, in criminal case, of evidence obtained by search by private individual*, 36 A.L.R.3d 553 (1971) (describing how evidence obtained by a private individual’s wrongful search may not be admitted based on Government involvement). Evidence retrieved as a result of an unreasonable search by a private party will not be admitted into evidence in a criminal prosecution against the victim of the search, if that search was “instigated or participated in by government agents.” *Id.*

31 See *Skinner*, 489 U.S. 602 at 615 (finding 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).

32 See U.S. v. Jacobsen, 466 U.S. 109, 115 (1984) (determining that if the government’s search exceeds the bounds of the private search, it is a separate search and the government is required to obtain a warrant or prove the search is necessary under another exigent circumstance); Walter v. U.S., 447 U.S. 649, 656–57 (1980) (reiterating the notion that “the Government may not exceed the scope of the private search unless it has the right to make an independent search.”); Alexandra Gioseffi, *LICHTENBERGER, SPARKS, AND WICKS: THE FUTURE OF THE PRIVATE SEARCH DOCTRINE*, 66 EMORY L.J. 395, 406 (2017) (explaining that if the Government’s search surpasses the limits of the private search, it is considered a separate, independent search).

33 See Gioseffi, *supra* note 32, at 399 (explaining that the private search doctrine allows government agents, without first obtaining a warrant, to reproduce a search previously performed by a private individual); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193, 233 (2005) (stating “[a] government search that merely replicates a previous private one is not a ‘search’ within the meaning of the Fourth Amendment search.”).
2. The Fourth Amendment in relation to Technology

When the Framers were contemplating the Constitution, the vast technological developments of modern day were not foreseeable. As a result, the jurisprudence of the Fourth Amendment has not clearly established the limitations of a “reasonable” search for governmental surveillance purposes in the context of personal devices and digital technologies. Traditionally, the two-pronged reasonable expectation of privacy test derived from *Katz v. United States* is used to determine whether a particular investigation constitutes a “search” under the Fourth Amendment. In *Katz*, the method of electronic surveillance was subjected to a constitutional analysis by including constructive intrusions and intangible appropriations in the definition of “search and seizure” under the Fourth Amendment. The Supreme Court ultimately expanded the Fourth Amendment to protect against unreasonable search and seizures involving electronic wiretaps, establishing that searches are not confined to only physical intrusion of personal property. The Court has also determined that a reasonable expectation of privacy exists if an individual does not consciously exposes private affairs to the public or knowingly

---

34 See Berk, *supra* note 23, at 3 (explaining the shortcomings of the Fourth Amendment in the context of unforeseen modern technology). It is clear that the drafters of the Fourth Amendment did not foresee “the nature of current information technology . . . .” *Id.* at 1. *See also* Russell L. Weaver, *THE FOURTH AMENDMENT, PRIVACY AND ADVANCING TECHNOLOGY*, 80 Miss. L. J. 1129, 1133 (2011) (recognizing that the Framers would not have known the effects that technology would have on the Fourth Amendment).

35 See Weaver, *supra* note 34, at 1138 (describing unclear standard for reasonableness of a search under the Fourth Amendment in light of technological advancements).


37 See *id.* at 353 (describing the definition of “search and seizure”).

38 See *id.* (expressing that searches are not limited to the physical context).
volunteers such information to third parties, such as private conversations in a public telephone booth.\footnote{See id. at 351 (stating matters that are “knowingly exposed to the public” remain unprotected).}

Historically, the two-pronged test has been utilized to determine whether evidence of surveillance is admissible in the context of criminal proceedings.\footnote{See Florida v. Riley, 488 U.S. 445, 450–51 (1989) (implementing the two-pronged test for analysis of an individual’s reasonable expectation of privacy).} The test has produced many instances where the technological evidence is admissible and does not infringe upon legitimate privacy concerns.\footnote{See id. (holding that aerial surveillance of a semi-covered greenhouse is not in violation of one’s reasonable expectation of privacy); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding a homeowner’s expectation of privacy was not violated when police used aerial surveillance from a high altitude of a fenced-in patio within the yard of a residence in the absence of a warrant to observe if marijuana was being grown); Dow Chem. Co. v. U.S., 476 U.S. 227, 239 (1986) (holding aerial photographs of a secure area surrounding an industrial facility otherwise unseen by the naked eye did not violate a reasonable expectation of privacy); U.S. v. Knotts, 460 U.S. 276, 285 (1983) (holding that the defendant had no legitimate interest of privacy when the police installed a beeper into a canister that sent signals to a radio receiver in an effort to observe the defendant’s location); U.S. v. Place, 462 U.S. 696, 706–07 (1983) (concluding that the utilization of a narcotic detection dog purposed for sniffing luggage does not intrude into the privacy interests of owners’ luggage); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the installation and use of a pen register did not violate the defendant’s expectation of privacy because dialed phone numbers are turned over to third parties). See also Andrew Guthrie Ferguson, \textit{Facial Recognition and the Fourth Amendment}, 105 MINN. L. REV. 1105, 1128–29 (2021) (noting several post-\textit{Katz} Supreme Court decisions concerning privacy rights to include digital technologies, representing a sense of flexibility in Constitutional analysis).} It has been found that an individual’s actual expectation of privacy is not reasonable to protect their bank records, telephone numbers they have dialed, and their private, fenced in areas.\footnote{See Oliver v. U.S., 466 U.S. 170, 176 (1984) (holding that trespassing on privately owned, fenced, open fields is not a search).} There are also many circumstances where similar evidence has not been deemed admissible based on a reasonable expectation of privacy.\footnote{See Carpenter v. U.S., 138 S. Ct. 2206, 2217 (2018) (holding that police accessing prior cell phone records showing past locations visited by the cell phone owner violates one’s expectation of privacy); Kyllo v. U.S., 533 U.S. 27, 40 (2001) (holding that one’s reasonable expectation of privacy is violated when a thermal imaging device is used by the police from street to detect heat from inside one’s home); U.S.}
invasion of privacy when technology is used to observe an individual while in the home. Based on the court’s inconsistent application of the Fourth Amendment for uses of technology, it is clear no conclusive rule has been formed as to when privacy rights have been infringed upon.

In decisions post-Katz, the court has combined privacy with property law concepts that have traditionally governed the Fourth amendment analysis, preventing the government from intruding upon private property by utilizing technological measures. A pivotal decision in Riley v. California essentially held that cell phones may be considered as private as the home under a Fourth Amendment analysis. This decision indicates that the Court acknowledges a

---

44 See James J. Tomkovicz, TECHNOLOGY AND THE THRESHOLD OF THE FOURTH AMENDMENT: A TALE OF TWO FUTURES, 72 Miss. L. J. 317, 396 (2002) (stating that information received about a private dwelling’s interior via technological methods will be protected by the Fourth Amendment despite the intimacy of the information or lack thereof). But see Katz v. U.S., 389 U.S. 347, 351 (1967) (recognizing that no Fourth Amendment protection applies when a person, while within their home, knowingly exposes private information to the public).

45 See Berk, supra note 23, at 11 (discussing the shortcomings of the court’s application of the Fourth Amendment to digital user data). The “extension of the Katz doctrine and the Stranger Principle to our current use of technology seems inconsistent with the interest underlying the Fourth Amendment.”

46 See Katz v. U.S., 389 U.S. 347, 351 (1967) (Harlan, J., concurring) (concluding that Fourth Amendment privacy protections are in place to protect the individual as opposed to mere places or objects). The court has clarified:

[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

47 See generally Riley v. California, 573 U.S. 373, 386 (2014) (holding that cell phones contain as much if not more personal information than the home). The Supreme Court’s holding does not immunize cell phone information from searches, but instead requires that such searches are done with a warrant even when the search is a result of a seizure incident to arrest. Prior to Riley, whether a warrant was required to search digital data was jurisdictionally split.
heightened interest in private digital information. Additionally, in *Carpenter v. United States*, where the government’s access of CSLI from a service provider was considered an invasion of the defendant’s reasonable expectation of privacy, the Court held that constituted a search for Fourth amendment purposes. Consequently, the government must generally obtain a search warrant pursuant to probable cause to access this type of data. Yet as new technology emerges, there are still many gaps that exist to determine the mechanisms the government may utilize to conduct searches upon citizens. Advancements in the digital era should not allow the government to defeat the protections of citizen’s privacy rights.

48 See Rani Molla, *People say they care about privacy but they continue to buy devices that can spy on them*, Vox (May 13, 2019), archived at https://perma.cc/Y4NK-BUVL (portraying the government’s substantial interest in digital data of individual’s for investigatory purposes).

49 See *Carpenter v. U.S.*, 138 S. Ct. 2206, 2220 (2018) (holding that CSLI is protected under the Fourth Amendment). The Court held that the unique qualities of cell phone location information insulate it from being subject to the “Third-Party Doctrine,” which typically allows the Government to access any information shared with a third party, per the logic that there is no reasonable expectation of privacy if the information is not kept private. *Id.* at 2217. Carpenter solidified that “whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.” *Id.*

50 See *id.* at 2221 (explaining that the government must generally obtain a search warrant to obtain an individual’s CSLI data).

51 See *Kyllo v. U.S.*, 533 U.S. 27, 40 (2001) (holding that use of thermal sensors to monitor a home violates an individual’s reasonable expectation of privacy); *U.S. v. Karo*, 468 U.S. 705, 716 (1984) (holding that the monitoring of a beeper in a private residence violates a reasonable expectation of privacy). In *Karo*, there was no infringement upon Fourth Amendment privacy rights because the beeper was inside a container, and it did not reveal information that could not have been obtained through visual surveillance of the naked eye. *Id.* at 707.

52 See Bagley, *supra* note 22, at 173 (arguing that data should be protected despite its location under the Fourth Amendment based on reasonableness expectation of privacy held by the user). Password-protected, encrypted digital storage containers should be a Fourth Amendment-protected place to store the “most intimate occurrences of the home.” *Id.* See Sagi Schwartzberg, *Hacking the Fourth: How the Gaps in the Law and Fourth Amendment Jurisprudence Leave the Right to Privacy at Risk*, 30 U. LA VERNE L. REV. 467, 485–86 (2009) (highlighting gaps of Fourth Amendment when applied to individual’s online data). See also John L. Potapchuk, *A Second Bite at the Apple: Federal Courts’ Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data*
III. Premise

As people have become increasingly dependent upon their personal devices, more and more personal data is being entrusted to private tech companies. The government has come to recognize the usefulness of this technology in relation to obtaining evidence in the course of criminal investigations. As a result, there has been legislative initiatives introduced by the government to coercively incentivize private companies such as Apple to aid law enforcement in the prevention of CSAM material by amending current legislation to broaden the liability of tech companies.

A. The Development of Legislation Imposing Liability on Tech Companies for User Conduct

Currently, there is no legislation explicitly compelling third party manufacturers to bypass the encryption of locked cell phones to provide access for the government. Federal legislation does not

Under the All Writs Act, 57 B.C. L. Rev. 1403, 1411 (2016) (discussing the dangers of intruding on user privacy rights by the wrongful use of technological advancements).

See Molla, supra note 48 (confirming the increased use of technology and data sharing by individuals in previous years). The “sales of smart devices increased 25 percent last year, according to marketing research firm IDC, and are expected to have double-digit growth for the next four years.” Id.

See Schwartzberg, supra note 52, at 469–70 (discussing the importance of digital data for evidentiary purposes and the government’s desire to obtain it from private tech companies). See also Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J. L. & Pol’y 211, 212 (2006) (highlighting the government’s intrusion of privacy rights for evidentiary purposes in criminal proceedings).


require private tech companies such as Apple to actively search for CSAM, but merely requires them to report known instances of it.\textsuperscript{57} As CSAM continues to increasingly be circulated online through personal technologies, the government has repeatedly attempted to enact legislation imposing increased liability on private tech companies for hosting the CSAM content of its users.\textsuperscript{58} Enacted under Title II of the Electronic Communications Privacy Act, Section 230 of the Communications Act (“Section 230”) protects tech companies from being held liable for the actions or content of their users.\textsuperscript{59} This law promotes online freedom of expression and the free flow of ideas via the internet.\textsuperscript{60} Section 230 also establishes the principle that the author of illegal, online content should be held responsible for their actions, not the platform that was used to host such content.\textsuperscript{61}

Congress attempted to amend Section 230 with the passing of the PROTECT Our Children Act in 2008, which created a reporting requirement for tech companies possessing "actual knowledge" of the (concluding current legislation being considered by the committee is still lacking and is still under advisement).

\textsuperscript{57} See 18 U.S. Code § 2258A (mandating tech companies to report known CSAM of users); U.S. v. Richardson, 607 F.3d 357, 366 (4th Cir. 2010) (holding private tech company AOL was not subject to a statutory scheme aside from its legal obligation to report known CSAM).


\textsuperscript{59} See 47 U.S.C.A. § 230 (limiting liability for online hosts based on content created by its users); \textit{Section 230 of the Communications Decency Act, ELEC. FRONTIER FOUND.} (Nov. 2021), archived at https://perma.cc/GF6K-2MRD (stressing the importance of Section 230 for the protection of innovation on the internet). Section 230 of the Communications Act states, “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” \textit{Id. See generally Melissa Medina, \textit{The Stored Communications Act: An Old Statute for Modern Times}, 63 AM. U. L. REV. 267, 270–71 (2013) (detailing a comprehensive account of the Act’s structure, applicability, and modern interpretation).}

\textsuperscript{60} See Felix T. Wu, \textit{Collateral Censorship and the Limits of Intermediary Immunity}, 87 NOTRE DAME L. REV. 293, 300 (2011) (noting speech-enhancing effects of Section 230 due to its preventing imposition of liability on intermediaries for harmful or offensive speech that they might otherwise censor).

\textsuperscript{61} See Jason Kelley, \textit{Section 230 is Good, Actually}, \textit{ELEC. FRONTIER FOUND.} (Dec. 3, 2020), archived at https://perma.cc/286K-TR8Q (underscoring that users should be held responsible for their own actions pursuant to Section 230).
presence of CSAM or child exploitation on their services. Soon after in 2020, Congress attempted to impose liability upon internet service providers for hosting sexually explicit material of children by introducing the amended EARN IT Act. After an amendment, the bill was introduced to the Senate in July of 2020 and a nearly identical bill was introduced to the House of Representatives shortly thereafter. The EARN IT Act contains a section entitled “No Effect on Child Exploitation Law”, which essentially strips private tech companies of their immunity from criminal and civil liability for hosting the illegal content of users granted by Section 230. The bill raised concerns regarding potentially negative effects on private tech companies, and it died in Congress in January, 2021.

The government has also attempted to mandate backdoor access to data stored on user’s cell phones. In 2020, these efforts


63 See Ahlam, supra note 58, at 837–38 (explaining the government’s motivation for amending Section 230 to impose liability on private tech companies for CSAM material). See also Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2020, S. 3398, 116th Cong. (2020) (introducing the EARN IT Act into Congress).


65 See, e.g., Joe Mullin, The New EARN IT Bill Still Threatens Encryption and Free Speech, ELEC. FRONTIER FOUND. (July 2, 2020), archived at https://perma.cc/G5YH-JIII (detailing the amended version of the EARN IT Act introduced to the Senate). “State lawmakers will be able to create new laws allowing private lawsuits and criminal prosecutions against Internet platforms, as long as they say their purpose is to stop crimes against children.” Id.

66 See Jericho Casper, Senate Judiciary Committee Teases, and Then Pulls, Bills Dramatically Narrowing Section 230 Protections, BROADBANDBREAKFAST (Jan. 2, 2021), archived at https://perma.cc/PX8K-94XB (discussing the implications of the EARN IT Act when the bill was about to die in Congress). “Critics of the EARN IT Act argue it is a misguided attack on internet speech, which would make it harder for online platforms to take common-sense moderation measures and shield only those which agree to confine their moderation policies to a narrowly tailored set of rules, agreed upon by legislators.” Id.

were continued when the more balanced Lawful Access to Encryption Data (“LAED”) Act was introduced, which essentially requires technology companies to create backdoor access to its devices.\(^68\) This bill was enacted to aid law enforcement agencies in detecting criminal behavior regarding matters of national security, such as the prevention of CSAM.\(^69\) The LAED Act requires private tech companies to assist law enforcement in accessing encrypted data from personal devices only after a court issues a warrant based on probable cause that a crime has occurred.\(^70\)

has attempted to mine user data from tech companies by seeking backdoor access to encrypted devices). \(\text{See also Andy Greenberg, Why Proposed State Bans on Phone Encryption Are Moronic, SLATE (Jan. 29, 2016) [hereinafter Bans on Phone Encryption Are Moronic] (disputing the proposition that law enforcement should be allowed backdoor access to encrypted data on user’s phones).}\)

\(^68\) \(\text{See Lawful Access to Encrypted Data Act, S. 4051, 116th Cong. (2020) (outlining the features of the EARN IT Act). "This bill requires certain technology companies to ensure that they can decode encrypted information on their services and products in order to provide such information to law enforcement." Id. See also Lawful Access to Encrypted Data Act, S. 4051, 116th Cong. § 3119 (2020) (defining “consumer electronic device” as a device that may be purchased by a member of the general public and one that contains more than 1 gigabyte of storage). See also Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity, COMM. ON THE JUD. (June 23, 2020), archived at https://perma.cc/2JTN-D2ZC [hereinafter LAED Balanced Solution] (explaining the backdoor access requirement of the LAED Act).}\)

\(^69\) \(\text{See Pfefferkorn, supra note 68 (signifying that the central purpose of the proposed bill is to have tech companies decrypt data for matters of national security). But see Ashcroft v. Free Speech Coal., 535 U.S. 234, 250 (2002) (explaining that not all legislation intended to prevent crime is justified when it suppresses an individual’s constitutional rights).}\)

\(^70\) \(\text{See LAED Balanced Solution, supra note 68 (describing the LAED Act and its balancing of interests). “The Lawful Access to Encrypted Data Act is a balanced solution that keeps in mind the constitutional rights afforded to all Americans, while}\)
B. Apple and User Data Privacy

Apple has consistently advertised itself as a tech company with a strong commitment to protect users’ private data from governmental intrusion. Tim Cook, the CEO of Apple, once wrote a letter to Apple users stating that Apple “respect[s] your privacy and protect[s] it with strong encryption, plus strict policies.” In 2014, Apple demonstrated its commitment to privacy by introducing a default encryption that almost guaranteed the company did not have the capability retrieve user data in compliance with a government search warrant. As a

providing law enforcement the tools needed to protect the public from everyday violent crime and threats to our national security.” Id.

71 See Apple’s Commitment to Customer Privacy, APPLE (June 16, 2013), archived at https://perma.cc/5YFM-HP7N (claiming that “[w]e do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order.”).

72 See Tim Cook, A Message to Our Customers, APPLE (Feb. 16, 2016), archived at https://perma.cc/ACW7-9BJA (explaining how Apple chose to protect the security of its customers when the government demanded certain tools to unlock user data). Tim Cook, Apple's CEO, argued that the government's request for a back door "would undermine the very freedoms and liberty our government is meant to protect." Id. See also Romain Dillet, Apple’s Tim Cook on iPhone unlocking case, TECHCRUNCH (Mar. 21, 2016), archived at https://perma.cc/K7LY-3ZJ4 (quoting Apple’s pledge, “we have a responsibility to protect your data and to protect your privacy . . . we will not shrink from this responsibility.”). See also Apple’s Commitment to Your Privacy, APPLE (Nov. 2021), archived at https://perma.cc/4Z8N-R3M4 (asserting Apple’s strong commitment to user privacy). “Privacy is a fundamental human right. At Apple, it’s also one of our core values.” Id.

73 See Benjamin Folkinshteyn, A Witness Against Himself: A Case for Stronger Legal Protection of Encryption, 30 SANTA CLARA HIGH TECH. L.J. 375, 378 (2014) (defining data encryption used by tech companies to protect user data). Encryption is defined as “a process by which the content of a particular message or document becomes unintelligible to a third party by a predesignated scrambling protocol.” Id. See also Kristin Finklea, CONG. RSCH. SERV., R44187, ENCRYPTION AND EVOLVING TECHNOLOGY: IMPLICATIONS FOR U.S. LAW ENFORCEMENT INVESTIGATIONS (2016) (underscoring Apple’s insistence that it is no longer “technically feasible” for the company to respond to government warrants for the extraction of this data.). The new iOS 8 system implemented by Apple protects users’ personal data via a passcode. Id. See also Alan Z. Rozenshtein, Surveillance Intermediaries, 70 STAN. L. REV. 99, 116 (2018) (describing how Apple continued to distinguish itself from its industry competitors by allowing iPhone users to opt-in to allow companies to track and collect usage data across apps). See User Privacy and Data Use, APPLE (Nov. 21, 2021), archived at https://perma.cc/AVV4-
result, Apple has claimed it is unwilling and unable to extract user data from a passcode locked iOS device because of the type of encryption used.\textsuperscript{74} Despite demands to implement end-to-end encryption of iCloud storage by privacy experts, Apple has refused to do so as a result of increased pressures from law enforcement.\textsuperscript{75} While Apple stakes its reputation as a protector of private information from the government, its terms of use state that it reserves the right to acquire “strategic partners” to share user information with.\textsuperscript{76}

The government has expressed concern that tech giants are taking excessive measures in order to strengthen privacy protections on personal devices.\textsuperscript{77} Criminal investigations can be hindered by law enforcement’s inability to access potentially vital data on users’ iPhone.\textsuperscript{78} Specifically, in 2016, the Federal Bureau of Investigation
(“FBI”) investigators attempted to compel Apple to unlock an iPhone belonging to a suspected shooter involved in a terrorist attack in San Bernardino, California. Apple refused the request based on the privacy concerns implicated if it allowed the government backdoor access to a locked, encrypted device. The FBI was granted a writ under the All Writs Act (AWA) by the district court, compelling Apple to assist in the execution of the search warrant. The government promptly withdrew its petition after Apple appealed the order, and later the government was able to hack the phone by other means.

Many service providers and device manufacturers continue refusing to cooperate with law enforcement to help recover encrypted data, even when presented with a lawful warrant supported by probable cause. Without that cooperation, law enforcement is left with few choices: attempt to hack into the encrypted data – at the expense of months, if not years, of lost investigative time plus the millions of dollars in funds needed to execute a hack – or abandon investigations altogether. As a result, our national security is at risk, and countless serious crimes committed in communities around the United States go unsolved.

Id. See also Leander Kahney, The FBI Wanted a Back Door to the iPhone. Tim Cook Said No, WIRED MAG. (Apr. 16, 2019), archived at https://perma.cc/NT53-76RJ (describing Apple’s refusal to allow the government backdoor access to suspect’s iPhone obstructed the investigation).

See Kahney, supra note 78 (recalling when Apple denied the government access to a criminal suspect’s iPhone without his consent).

See Dillet, supra note 72 (explaining Apple’s refusal to allow government backdoor access to data based on user’s reasonable expectation of privacy in the data); Ahlam, supra note 58, at 789 (stating that Apple refused to comply with government’s request to decrypt the suspect’s smartphone because it did not possess the decryption key). “Further, Apple refused to comply with requests to write code to allow for backdoor access, citing privacy and cybersecurity concerns.” Id.

See 28 U.S.C. § 1651 (2012) (allowing courts to issue all writs necessary in order to assist with its respective, lawful objective); Eric Lichtblau, Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman, N.Y. TIMES (Feb. 16, 2016), archived at https://perma.cc/B7DJ-65XD [hereinafter Judge Tells Apple to Help Unlock iPhone] (detailing the California judge’s request for Apple “to provide ‘reasonable technical assistance’ to the F.B.I.” in unlocking the suspect’s phone).

See also Tim Limer, Most Useful Podcast Ever: Why Is the FBI Using a 227-Year-Old Law Against Apple?, POPULAR MECHANICS (Feb. 24, 2016), archived at https://perma.cc/2AJX-WSRX (explaining the All Writs Act and the government’s attempts to use it to force tech companies into compliance with investigations of consumers).

See Katie Benner & Eric Lichtblau, U.S. Says It Has Unlocked iPhone Without Apple, N.Y. TIMES (Mar. 28, 2016), archived at https://perma.cc/KXB2-3YUR [hereinafter U.S. Says It Has Unlocked iPhone Without Apple] (stating the
C. Apple’s Newly Proposed CSAM Prevention Feature

Apple has proposed three new features to combat the spread of CSAM material. The first, and most controversial, involves a tool that automatically scans photos stored on users’ Apple devices before they are uploaded to iCloud. Those images are then compared with NCEM’s database of child sexual abuse images to determine if there is a match. The matches will only be decrypted if there are multiple matches to ensure there is an entire collection of CSAM being detected. If the threshold number of matches for known CSAM content is exceeded, Apple will then manually review the images reported to confirm a positive match. If a match is confirmed, the user’s account is disabled and Apple will subsequently send a report to NCMEC. After the announcement of the newly proposed feature, Apple released a statement addressing numerous concerns where the government found an alternative method to unlock the suspect’s iPhone, leading to the withdrawal of its previous legal tactic designed to compel Apple’s assistance.

83 See Expanded Protections for Children, APPLE (Sept. 3, 2021), archived at https://perma.cc/D7J5-D4YL [hereinafter Expanded Protections for Children] (discussing the three new features Apple is planning on rolling out with its next software).

84 See Sarit K. Mizrahi, The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users During the Course of Criminal Investigations in Canada and the United States, 25 TUL. INT'L & COMPAR. L. 303, 304 (2017) (explaining that cloud computing technology allows individuals to remotely store and access data). User data stored in iCloud, a cloud computing system, subjects an individual’s data to be stored alongside the data of various users that are unknown to one another. Id.

85 See id. (highlighting the safeguards Apple has implemented to prevent matches that are false positives).

86 See Expanded Protections for Children, supra note 83 (explaining the accuracy that the threshold provides in order to ensure accuracy when flagging accounts).

87 See id. (establishing the consequence of a positive CSAM match detection).
company insisted that the system was designed with user privacy in mind.\textsuperscript{89}

\textbf{D. Government Agents and entities}

\textbf{1. NCMEC is a Government Agent or Entity}

NCMEC was established in 1984 by the United States Congress, and advertises itself as a private, nonprofit organization dedicated to preventing the spread of material sexually exploiting children.\textsuperscript{90} Many tech companies have sent NCMEC reports of child abuse flagged on their platforms and devices.\textsuperscript{91} As such, for a long period of time, the private organization had been able to conduct searches through people’s private files and documents sent to them as they saw fit.\textsuperscript{92} Eventually in August of 2016, the Tenth Circuit was faced with deciding whether NCMEC constitutes a private corporation as

\textsuperscript{89}See id. (outlining the technology utilized to protect privacy interests of users while assisting law enforcement in detecting CSAM material stored on user devices). Apple clarified that the technology still provides “significant privacy benefits over existing techniques since Apple only learns about users’ photos if they have a collection of known CSAM in their iCloud Photos account.” Id. “Instead of scanning images in the cloud, the system performs on-device matching using a database of known CSAM image hashes provided by NCMEC and other child safety organizations.” Id. See also Expanded Protections for Children Frequently Asked Questions, APPLE (Aug. 2021), archived at https://perma.cc/CVN6-8FUR [hereinafter Frequently Asked Questions] (addressing user privacy concerns and explaining the features in depth).

\textsuperscript{90}See Our Work, supra note 6 (highlighting that although NCMEC claims the government exerts no control over the organization’s website, the organization is partially funded “through a grant from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice.”).

\textsuperscript{91}See Anirudh Krishna, Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse, 109 CAL. L. REV. 1581, 1603–05 (2021) (using Facebook as an example of a platform that sends flagged content to NCMEC). “In 2019, NCMEC received over sixty-nine million reports of CSAM, many of them from tech platforms like Google and Facebook.” Id. at 1586.

\textsuperscript{92}See John Floyd, National Center for Missing & Exploited Children Is a Government Agent For Fourth Amendment, Search and Seizure Purposes, JOHN T. FLOYD L. FIRM (Aug. 12, 2016), archived at https://perma.cc/U5FY-Q5GH (explaining that private individuals are not subject to the Fourth Amendment jurisprudence for search and seizures). “The U.S. Supreme Court has long established that a search and seizure by a private individual or entity does not enjoy Fourth Amendment protections, unless the private actor is acting as an agent of the government.” Id.
opposed to a governmental entity or agent for Fourth Amendment purposes.\footnote{93 See U.S. v. Ackerman, 831 F.3d 1292, 1296–97 (10th Cir. 2016) (deciding if NCMEC should be labeled a government agent for Fourth Amendment purposes).}

On the appeal in \textit{United States v. Ackerman} ("Ackerman II"), the United States Court of Appeals for the Tenth Circuit held that NCMEC was a government entity acting as an agent of the government, and that its unwarranted search of the defendant’s emails implicated the Fourth Amendment.\footnote{94 See id. (finding that NCMEC’s mandate by federal statute to collaborate with federal and local law enforcement, among other privileges beyond that of a private person, qualifies NCMEC as a governmental entity).} Significantly, the court noted that the organization is governed by statute requiring it to 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 [\textit{Lebron}]."\footnote{95 See id. at 1298 (listing the multiple daily functions mandated by statute).} It was also reasoned that NCMEC was afforded “many unique law enforcement powers” that private individuals were not, which contributed to its rightful status as a governmental entity.\footnote{96 See id. at 1298 n.4 (citing to \textit{U.S. v. Keith}, 980 F. Supp. 2d 33, 41 (D. Mass. 2013)) (reasoning that NCMEC has privileges beyond what the ordinary citizen is granted).} The court went on to find that even if NCMEC had not qualified as a government entity, it still was acting as an agent of the government for Fourth Amendment purposes.\footnote{97 See id. at 1308 (holding that NCMEC ultimately must be seen as an agent of the government when searching through the defendant’s emails).} As the courts in \textit{Skinner} and \textit{Ackerman II} made clear, the simple existence of independent motivation for the private search, such as financial gain, does not defeat a finding of government action.\footnote{98 See \textit{Ackerman}, 831 F.3d at 1301 (holding that “[n]either 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).”). The Court pointed out that “agents routinely intend to serve their principals with the further intention to make money for themselves.” \textit{Id.} at 1303.} Therefore, NCMEC’s independent reasons for investigating CSAM did not solely defeat the notion that it was a government agent.\footnote{99 See id. at 1301 (rejecting the argument that NCMEC should not be considered a government agent because the organization had its own objectives independent from governmental objectives).} The aftermath of the
Ackerman II decision has allowed and increasing number of courts to accept the conclusion that NCMEC is a government agent or entity.\textsuperscript{100}

2. Tech Companies and Government Agent Status

Courts have not ruled out the possibility that private tech companies such as Apple can act as government agents under the right circumstances.\textsuperscript{101} There have been instances where certain actions taken by tech companies were examined under a Fourth amendment analysis.\textsuperscript{102} For example, the court in United States v. DiTomasso reasoned that the tech companies Omegle and AOL could constitute government agents despite having independent reasons for scanning the defendant’s emails for CSAM content.\textsuperscript{103} The court emphasized that the material question to be resolved was whether the defendant had consented to the search when he signed the companies’ terms and services agreement.\textsuperscript{104} The court concluded that the defendant did consent to AOL terms and services where it was made clear the platform would work with law enforcement if it found illegal activity, but he did not consent to Omegle terms and services because it was not evident the company would work with law enforcement in response to

\textsuperscript{100} See, e.g., U.S. 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); U.S. v. Powell, 925 F.3d 1, 6 (1st Cir. 2018) (introducing the Fourth Amendment analysis with the assumption that “for all relevant purposes” NCMEC was acting as a government agent when it viewed the CSAM material reported by the private tech company Omegle).

\textsuperscript{101} See U.S. v. DiTomasso, 56 F. Supp. 3d 584, 596 (S.D.N.Y. 2014) (assuming tech companies Omegle and AOL could act as government agents even if they had independent reasons for scanning the defendant’s emails and chats for child pornography).

\textsuperscript{102} See id. at 596–97 (analyzing the searches of the defendant’s accounts performed by Omegle and AOL under the Fourth Amendment).

\textsuperscript{103} See id. (examining different terms of service agreements of AOL and Omegle and confirming the companies’ role as government agents for Fourth Amendment purposes).

\textsuperscript{104} See id. at 591 (reasoning that consent is proper if a user signs the term and agreement of services with the understanding that his data will be shared). The court held that the test to determine whether an individual consented to a Fourth Amendment search is “an ‘objective’ question: it depends on how ‘the typical reasonable person [would understand]’” the conduct supposedly amounting to consent. Id.
such activity. This holding suggests the possibility that tech companies will be considered government agents subject to a Fourth Amendment analysis, and this potentially may turn on the specific language used in the terms and services agreements.

IV. Analysis

This section identifies the primary concerns associated with private tech companies’ implementation of spyware technologies to aid government objectives, identifies the shortcomings of past failed federal regulatory legislation, and recommends stronger privacy protections to mitigate potential abuse by the government and their agents.

A. Constitutional Concerns Regarding the Invasion of Privacy and Fourth Amendment Violations

The proposed new CSAM feature presented by Apple poses the question as to whether the private tech companies’ relationship with law enforcement presents a constitutional violation of privacy under the Fourth Amendment jurisprudence. As the expansion of technology has advanced well beyond what established law anticipated concerning tech companies access and dissemination of an individual’s private, digital information, there is currently no clear legislative restriction to such access. This determination is made by

105 See id. at 597 (holding that the defendant’s consent to AOL’s terms of service constituted a waiver of his Fourth Amendment rights).
106 See DiTomasso, 56 F. Supp. 3d at 588 (outlining AOL’s terms of use that users are required to assent to and how the company made clear it would report illegal behavior by users to law enforcement).
107 See discussion infra, Sections IV A–B (providing examples of the negative implications of Apple’s access to user data for government purposes in the first section and criticizing and modifying past legislative proposals in the latter).
108 See Reed, supra note 4 (acknowledging that Apple’s new surveillance technology utilized in compliance with law enforcement may constitute a violation of the Fourth Amendment).
109 See Schwartzberg, supra note 52, at 474 (describing how the Fourth Amendment and the complex issues technology presents when applying this provision). “Changing technology has caused much confusion in the interpretation of the Fourth Amendment.” Id. See also Mizarhi, supra note 84, at 324 (describing the lack of definitive legislation or court precedent affirming protections for user data entrusted
the tech companies themselves, and therefore Apple’s decision to acquire and disseminate certain user information must be analyzed to understand the dangers of sacrificing user privacy for the purpose of assisting law enforcement.\textsuperscript{110}

Privacy and security experts have consistently cautioned against any legislatively mandated "back door" because it would materially weaken security as well as privacy protections.\textsuperscript{111} In this respect, Apple has promised it will refuse government “demands to build and deploy government-mandated changes that degrade the privacy of users.”\textsuperscript{112} Although Apple insists that all other user data is still unreachable, the system itself is proof that the company is able to

\textsuperscript{110} See Reed, supra note 4 (highlighting the privacy problems associated with Apple’s proposed new feature to prevent CSAM). See also Brenner & Clarke, supra note 54, at 248 (considering the relationship between Government interests and societal expectations of privacy). “Although the purpose of the Fourth Amendment is to promote reasonable Government action, even reasonable Government action is subordinate to society's interest in honoring generally accepted expectations as to what is, and what is not, private.” Id.

\textsuperscript{111} See Reed, supra note 4 (stating “Apple’s announcement was immediately denounced by technology, cybersecurity and privacy advocates.”).

All it would take to widen the narrow backdoor that Apple is building is an expansion of the machine learning parameters to look for additional types of content, or a tweak of the configuration flags to scan, not just children’s, but anyone’s accounts. That’s not a slippery slope; that’s a fully built system just waiting for external pressure to make the slightest change. Id. See also Potapchuk, supra note 52, at 1411 (describing the dangers associated with requiring tech companies to build backdoor access to user data on encrypted devices). See, e.g., Bans on Phone Encryption Are Moronic, supra note 67 (criticizing law enforcement’s encouragement for laws mandating access to encrypted devices for criminal investigation purposes).

\textsuperscript{112} See Frequently Asked Questions, supra note 89 (assuring Apple users that the company will not allow the government to take advantage of user data due to government-mandated changes). Apple claims in the past the company has “steadfastly refused those demands. We will continue to refuse them in the future. Let us be clear, this technology is limited to detecting CSAM stored in iCloud and we will not accede to any government’s request to expand it.” Id.
create a backdoor into user data allowing for third party access.\textsuperscript{113} It is clear that the company has the capability to scan all photos uploaded and privately stored to iCloud despite whether users have an actual, subjective expectation of privacy and such an expectation is reasonable based on society’s standards in the digital age.\textsuperscript{114}

Advocates for a more limited application of the Fourth Amendment argue there can be no reasonable expectation of privacy in information when it is stored on electronic devices that a third party is able to acquire access to.\textsuperscript{115} Although the Third-Party Doctrine is still good law, the ruling in Carpenter narrows this concept by providing that certain shared information holds a heightened expectation of privacy because the individual did not consciously assume the risk that the third party holding their private data would share this information with the government.\textsuperscript{116} In Carpenter, the court held that all cell phone users did not assume the risk of sharing their location data, which is protected by the Fourth Amendment.\textsuperscript{117} Generally in these instances, the government does not have the lawful ability to access this type of information without a warrant for the purpose of a criminal investigation.\textsuperscript{118} While the objective is in the

\textsuperscript{113} See Schoen, supra note 67 (warning against the use of backdoors in software due to unprecedented privacy breaches). When companies and legislature require deliberate backdoors, security is weakened as it “amounts to developing for our adversaries’ capabilities that they may not have the competence, access or resources to develop on their own.” Id.

\textsuperscript{114} See Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (featuring a two-pronged analysis to establish whether a person has a privacy interest). The Court determined that “there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” Id.

\textsuperscript{115} See Schwartzberg, supra note 52, at 487 (commenting that some experts hold the opinion that the Fourth amendment cannot apply to internet services). “At least one commentator has suggested that the Fourth Amendment may never be applicable when the Internet is involved because ‘the Fourth Amendment does not protect information that has been disclosed to third-parties, and the [I]nternet works by disclosing information to third parties.’” Id.

\textsuperscript{116} See Carpenter v. U.S., 138 S. Ct. 2206, 2218 (2018) (modifying the Third-Party Doctrine to emphasize that cell it is not reasonable for phone users to expect that their location data is being shared with the government).

\textsuperscript{117} See id. at 2217 (holding that cell phone users did not assume the risk of sharing CSLI data).

\textsuperscript{118} See id. (holding that CSLI data falls outside the reach of the Third-Party Doctrine). See also Overview of the Fourth Amendment, supra note 13 (explaining there is a
interest of promoting public welfare, this cannot justify stripping away
the constitutional protections in place that create privacy zones
expected to be free from government intrusion in the absence of
probable cause, a warrant, or a warrant exception.\textsuperscript{119} In the digital age,
allowing the government access through Apple, a private party hosting
user data, undermines any sufficient degree of protection for innocent,
privately stored information that unaware users maintain on their
personal devices.\textsuperscript{120} If the government is granted such a generalized
access to search for CSAM with the coerced compliance of Apple, this
loophole will undermine the purpose of the Fourth Amendment
protections because it is inconsistent with the overall intent to protect
private data or effects.\textsuperscript{121}

\textsuperscript{119} See Carpenter, 138 S. Ct. at 2217 (holding that “[a] person does not surrender all
Fourth Amendment protection by venturing into the public sphere.”). The Court’s
decision regarding law enforcement’s use of historic cell-site location information
expressed the notion that to “secretly monitor and catalogue every single movement”
of an individual constituted a violation of society’s expectations about the scope of
law enforcement’s authority. \textit{Id.}

(applying the Third-Party Doctrine to more modern digital scenarios).
People disclose the phone numbers that they dial or text to their cellular
providers, the URLs that they visit and the e-mail addresses with which they
correspond to their Internet service providers, and the books, groceries and
medications they purchase to online retailers [ ... ] But whatever the societal
expectations, they can attain constitutionally protected status only if our
Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite
for privacy. I would not assume that all information voluntarily disclosed
to some member of the public for a limited purpose is, for that reason alone,
disentitled to Fourth Amendment protection. \textit{Id. See also} Brenner & Clarke, \textit{supra} note 54, at 248 (analyzing the “subjective”
element of the \textit{Katz} test). The subjective factor is evaluated based upon the “facts
and circumstances known to the Consumer.” \textit{Id.}

\textsuperscript{121} See Berk, \textit{supra} note 23, at 1 (comparing the original intent of the Fourth
Amendment in privacy protections with present digital data concerns). See also
legislation is justified when a constitutional right is infringed upon). “While the
Government asserts that the images can lead to actual instances of child abuse . . .
The harm does not necessarily follow from the speech.” \textit{Id. See also} Brenner &
Clarke, \textit{supra} note 54, at 246–47 (predicting the inadequacies of the Fourth
Amendment in terms of twenty-first century technologies). “[A]s computer
technology becomes more embedded in society, consumers will be increasingly
B. The EARN IT Act and Similar Legislation Transforms Apple into a Government Agent

If proposed legislation such as the EARN IT Act is implemented, Apple and other private tech companies pursuing governmental objectives must be considered agents of the government, and all searches conducted as such are subject to the protections of the Fourth Amendment. 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. The government must also “[do] more than adopt a passive position toward the underlying private conduct.” Pursuant to the proposed EARN IT legislation, it is clear that the government is encouraging and endorsing Apple and other tech companies into conducting searches on their behalf to prevent criminal activity. Apple has succumbed

forced to waive their Fourth Amendment rights in order to obtain vital goods and services.” Id. at 245–46.

See Casper, supra note 66 (describing the shortcomings of the EARN IT Act).
See also Vallee & Azarmi, supra note 5 (emphasizing the legal significance of the government mobilizing private actors to search for CSAM).

[I]f a private party becomes an agent of the government who conducts searches for the government, the Fourth Amendment applies to those searches. When a search is conducted without a warrant required by the Fourth Amendment, the information seized from that unconstitutional search is properly excluded from evidence – and when it is the basis for a CSAM prosecution, the prosecution can be dismissed. And in the case of EARN IT, any mandate for a company to search through a consumer’s content would violate the warrant requirement, and therefore not be usable in court.

Id.


See id. (revealing that the government recruits a private party as its agent when they take coercive measures to encourage the third party action). See also U.S. v. Miller, 425 U.S. 435, 443 (1976) (holding that a private party can still be an agent of the government if the party performing the search intended to assist law enforcement initiatives).

See Wakabayashi, supra note 55 (asserting lawmakers are threatening to amend Section 230 in order to compel tech companies to assist the government in regulating indecent material on the internet).
to such governmental pressures, similar to the circumstances seen in *Skinner*, with the rollout of its CSAM prevention features.\(^{126}\)

Even if Apple is not coerced by legislation into searching for and reporting CSAM to the government and decides to do so voluntarily in spite of its historical devotion to user privacy, this action should still invoke the government agency analysis under the Fourth Amendment because Apple would be working directly with NCMEC, a government agent.\(^{127}\) As the court has held in *Ackerman II*, NCMEC is a government agent pursuant to its CSAM prevention initiatives and close collaboration with the government.\(^{128}\) Apple’s collaboration with a government agent such as NCMEC regarding iPhone user information broadens the Third-Party Doctrine beyond its intended scope, as all iPhone users likely do not assume their information will be scanned and shared with the US government or its agents for any purpose.\(^{129}\) If tech companies such as Apple are strongly encouraged

\(^{126}\) See Reed, *supra* note 4 (criticizing Apple’s submission in aiding law enforcement for CSAM purposes and putting user privacy at risk).

The going over of Apple to the undemocratic policies of the entire American political and law enforcement establishment is predictable. The massive corporate monopoly and number one entity on Wall Street—with a staggering $2.4 trillion market valuation—is incapable of maintaining even a fig leaf of adherence to democratic rights and defending the Fourth Amendment guarantee against unreasonable searches and seizures.

\(^{127}\) See U.S. v. Ackerman, 831 F.3d 1292, 1302 (10th Cir. 2016) (finding NCMEC to be a government agent when implementing the Fourth Amendment analysis); U.S. 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); U.S. v. Powell, 925 F.3d 1, 5 (1st Cir. 2018) (introducing the Fourth Amendment analysis with the assumption that “for all relevant purposes” NCMEC was acting as a government agent when it viewed the CSAM material reported by the private tech company Omegle).

\(^{128}\) See *Ackerman II*, 831 F.3d at 1301 (holding that NCMEC’s mandate by federal statute to collaborate with federal and local law enforcement, among other privileges beyond that of a private person, qualifies NCMEC as a governmental entity). See also *Skinner*, 489 U.S. at 614–16 (finding 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).

\(^{129}\) See *Katz* v. U.S. 389 U.S. 347, 351–52 (1967) (discussing how telephone technology has become a vital to private communications).

[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection... But what he seeks to preserve
by the government or its agents to freely access and share user data for the purpose of CSAM prevention, it is imperative that the courts or legislation protect fundamental user privacy concerns by finding these searches unconstitutional under the Fourth Amendment.130

V. Conclusion

The Fourth Amendment was intended to protect a citizen’s reasonable expectation of privacy, a notion that has not been as easily transferable in protecting an individual’s technological data. Society has become increasingly reliant on Apple and other tech companies, which has led to individuals entrusting these entities with personal information. Therefore, the government will continue its efforts to coerce Apple and others into handing over valuable personal data for its own surveillance purposes. This type of intrusion is what the Fourth Amendment was designed to protect against, and technological

as private, even in an area accessible to the public, may be constitutionally protected.

Id. See also Vallee & Azarmi, supra note 5 (attempting to shed light on user privacy concerns relating to scanning systems used by private tech companies). “It is impossible to guarantee that a scanning system will only be used to detect CSAM, and not also expanded to attempt to detect terrorist or other extremist content.” Id. See also Goldman, supra note 25 (alleging that the protections of the Fourth Amendment should be interpreted in a way that is up to date with modern technology). See also Berk, supra note 23 (stressing the shortcomings of the Fourth Amendment in terms of the right to privacy in data stored in the cloud).

Current Fourth Amendment jurisprudence, therefore, could treat all this information as unprotected, as a simplistic application of the Stranger Principle entails that information put into a third party's hands is not intended to, nor reasonably expected to be, maintained as private. But that appears wrong. The security protected by the Fourth Amendment should include the security of the data we generate, whether we permit that data to be held by and collected by a third party, or whether we hold it and collect it ourselves.

Id.

130 See Berk, supra note 23 (underscoring the importance of reevaluating current legislation and protections for individual’s right to privacy in the technological age). “... [T]he use of information technologies vastly increases the scope and possibility of governmental and private parties' interference with and surveillance of individuals, and, as a result, creates severe tensions on the jurisprudential theories used to protect basic liberties and privacies.” Id.
advancements cannot be used as a tool to escape one’s reasonable expectation of privacy in one’s personal information stored on a cellphone. Additionally, the Third-Party Doctrine should be limited in scope when tech companies work with organizations such as NCMEC—who have been deemed a government agent. If safeguards such as a warrant requirement are not upheld, the government will be permitted to justify any intrusion into user data as long as it is accompanied by an attenuated, morally acceptable objective. Despite Apple’s worthy goal of preventing the spread of CSAM, employing a mechanism to decrypt user data for the purpose of sharing such information with the government and its agents constitutes a search and seizure under the Fourth Amendment in the digital era, and should therefore be subject to its protections.