WALLING OFF PRIVACY:

APPLE'S NEURALHASH CONTROVERSY, THE ECPA, THE FOURTH AMENDMENT, AND ENCRYPTION

GABRIEL J. RUDIN*

[*] J.D., University of Colorado Law School, Class of 2023. I would like to thank Amie Stepanovich, Professor Margot E. Kaminski, Professor Benjamin Levin, and Riana Pfefferkorn for their insights and expertise. All mistakes are my own.

In August of 2021, Apple announced a series of controversial features for its iPhone iOS 15 operating system designed to combat the spread of child sexual abuse material (CSAM). Two of the most notable features included: (1) client-side scanning of photos stored within the iCloud Photos application and (2) content moderation of user communications within the Messages application. Many privacy advocates raised serious concerns over the processes Apple proposed and the possibility of exploiting this technology for other ends—"function creep"—with a potential chilling effect on associative freedoms more generally. These concerns require re-examining the uneasy relationship between the Fourth Amendment and the Electronic Communications Privacy Act (ECPA) to fully understand what makes these features so controversial in addition to analyzing Apple's proposed technologies in detail. This note does not take issue with combating the spread of CSAM through technological means. Rather, it seeks to explain why concerns about Apple's proposed features, in particular, are justified. It explores how Apple's proposed safety features could undermine individuals' reasonable expectation of privacy (REP) in their smartphone devices and electronic communications, as well as potentially create opportunity for further judicial inconsistencies. Finally, it proposes a new framework as an attempt to address these multifaceted issues: that the Supreme Court recognize the encryption of communications, data and files from personal smartphone devices as akin to the walls of one's home in a search context. This metaphor helps harmonize the ECPA's and the Fourth Amendment's different oversight requirements to reinforce individuals' REP in electronic communications and smartphone devices.

INTRODUCTION

In August of 2021, Apple announced new safety features for its iPhone iOS15 operating system designed to combat the spread of child sexual abuse materials (CSAM).[1] Most notably, the new features included: (1) a proprietary CSAM detection algorithm, NeuralHash, that performs on-device (client-side) scanning of users' images that are uploaded into iCloud Photos and (2) various mechanisms for moderating the content of user communications within the Messages application (Messages app).[2] The rollout of these plans was initially delayed following intense public backlash.[3] Then, in December of 2022, Apple decided after "extensive consultation with experts"[4] to abandon NeuralHash and double-down on the content moderation systems integrated in its Messages app to interrupt the CSAM cycle before it occurs.[5] The arc of this saga offers a unique case study into sophisticated technological capabilities, business judgment, and shifting corporate policies. Despite being shelved, the NeuralHash feature remains important to evaluate post-cancellation because it utilized client-side scanning on end-users' devices, which is different in kind from other major companies'[6] CSAM-targeting scanning in the cloud (server-side).

First and foremost, this note does not argue against combating the spread of CSAM. Instead, it evaluates whether Apple's new safety features would undermine individuals' reasonable expectations of privacy (REP) in their cell phone devices.[7] In doing so, it illustrates a need to harmonize the Fourth Amendment's minimum

[1] *See* Frank Bajack & Barbara Ortutay, *Apple to scan U.S. iPhones for Images of Child Sexual Abuse*, AP NEWS (Aug. 6, 2021), https://apnews.com/article/technology-business-child-abuse-apple-inc-7fe2a09427d663cda8addfeeffc40196 [https://perma.cc/44M4-HJ55].

[2] Apple announced three updates in total; this paper focuses on the two most controversial updates. Matthew Panzarino, *Interview: Apple's Head of Privacy Details Child Abuse Detection and Messages Safety Features*, TECHCRUNCH (Aug. 10, 2021, 9:00 AM), https://techcrunch.com/2021/08/10/interview-apples-head-of-privacy-details-child-abuse-detection-and-messages-safety-features/ [https://perma.cc/BGZ3-XTT3].

[3] *See* Cindy Cohn, *Delays Aren't Good Enough—Apple Must Abandon Its Surveillance Plans*, ELEC. FRONTIER FOUND. (Sept. 3, 2021), https://www.eff.org/deeplinks/2021/09/delays-arent-good-enough-apple-must-abandon-its-surveillance-plans [https://perma.cc/JY3A-YJMV].

[4] Lily Hay Newman, *Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next*, WIRED (Dec. 7, 2022, 1:11 PM), https://www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages/ [https://perma.cc/Z55G-PX4L].

[5] *Id.*; *see* Robert McMillan et al., *Apple Plans New Encryption System to Ward Off Hackers and Protect iCloud Data*, WALL ST. J. (Dec. 7, 2022, 8:47 PM), https://www.wsj.com/articles/apple-plans-new-encryption-system-to-ward-off-hackers-and-protect-icloud-data-11670435635 [https://perma.cc/Z55G-PX4L].

[6] *See* Jon Callas, Thoughts on Mitigating Abuse in an End-to-End World 6 (Stanford Internet Observatory's End-to-End Encryption Workshop Series, 2020), https://cyber.fsi.stanford.edu/io/events/crypto-e2ee-workshop [https://perma.cc/WU9J-RXEH].

[7] This paper uses the terms "cell phone" and "smartphone" interchangeably.

level of protection (a probable cause warrant) with the variable judicial oversight requirements provided in the ECPA, which are less stringent in some circumstances. Apple's announcement will require the judiciary to reconsider how the Fourth Amendment and the ECPA interact with one another due to the complexity of modern cell phones. In turn, this note proposes that the Supreme Court should view the encryption of electronic files as akin to the physical walls of one's home. The Court's application of this metaphor would help harmonize the ECPA's statutory regime with the Fourth Amendment's minimum constitutional protections and, ultimately, reinforce individual privacy interests in the contents of their electronic communications and smartphone devices.

Part I of this note discusses the technical aspects behind Apple's proposed safety features and privacy advocates' concerns. Then, Part II discusses the applicable sources of law implicated in Apple's proposal. Part III explores iPhone users' ownership interests in data stored on their devices, the Apple Privacy Policy, and the terms and conditions of the Apple iOS15 Software License Agreement (referred to as the "User Agreement"). Finally, Part IV encourages the Supreme Court to treat encrypted smartphone data akin to as the physical walls of one's home in a search context.

I. APPLE'S NEURALHASH CONTROVERSY

A. *Combating the Spread of CSAM Online Versus Protecting Privacy Rights*

Reducing the proliferation of CSAM while protecting individual privacy makes for a difficult balancing act.[8] Due to the criminal nature of child abuse and troubling increase of CSAM,[9] law enforcement must strive to protect children to the greatest extent possible. However, some commentators express concern that means used to combat CSAM proliferation, such as weakening encryption and client-side scanning, may jeopardize individuals' privacy rights.[10] This skepticism puts privacy activists in an uncomfortable position seemingly devoid of nuance—a tension that compounds the harm of

[8] *See, e.g.*, Newman, *supra* note 4 ("Countering CSAM is a complicated and nuanced endeavor").

[9] *See* Patricia Davis, *100,000,000 The Race to Save Children Behind the Staggering Number*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN BLOG (Dec. 1, 2021), https://www.missingkids.org/blog/2021/100,000,000-the-race-to-save-children-behind-the-staggering-number [https://perma.cc/9ABJ-9WVV].

[10] *See, e.g.*, Tiffany C. Li, *Apple's CSAM Prevention Features Are a Privacy Disaster in the Making*, MSNBC (Aug. 12, 2021, 11:20 AM), https://www.msnbc.com/opinion/apple-s-csam-prevention-features-are-privacy-disaster-making-n1276607 [https://perma.cc/UW33-5HJG].

these evils by stymieing a necessary dialogue about privacy rights in society. Although the tireless pursuit of criminals is necessary, we should be mindful of Justice Brandeis' words of wisdom:

> [e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[11]

The uncomfortable tension between privacy and security lies at the heart of this paper. It is perhaps most poignant in circumstances where legal doctrine, statutes, and constitutional rights overlap or conflict.[12]

B. Apple's Reputation as a Privacy Advocate

Apple holds itself out as a zealous advocate of privacy rights.[13] It has purchased billboards and run national advertising campaigns centered around its commitment to privacy.[14] As of this writing, for example, Apple's website proudly states: "Privacy is a fundamental human right. At Apple, it's also one of our core values. Your devices are important to so many parts of your life. What you share from those experiences should be up to you."[15]

Apple has a history of prioritizing privacy rights above countervailing societal interests: for example, Apple's highly-publicized legal battle with the Federal Bureau of Investigation (FBI) after the

[11] Olmstead v. United States, 277 U.S. 438, 479 (1928).

[12] *See generally, e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011); *see also* Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RSCH. CTR. (Feb. 19, 2016), https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ [https://perma.cc/7VT4-6JVH].

[13] *See* Kif Leswing, *Apple Is Turning Privacy into a Business Advantage, Not Just a Marketing Slogan*, CNBC (June 7, 2021, 6:52 PM), https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business-advantage.html [https://perma.cc/3788-KYFA].

[14] *See* Chance Miller, *Ahead of CES Apple Touts 'What Happens on Your iPhone, Stays on Your iPhone' with Privacy Billboard in Las Vegas*, 9TO5MAC (Jan. 5, 2019, 6:03 AM), https://9to5mac.com/2019/01/05/apple-privacy-billboard-vegas-ces/ [https://perma.cc/BK9C-YDLN].

[15] *Privacy*, APPLE, https://www.apple.com/privacy/ (last visited July 8, 2023) [https://perma.cc/84B6-L7EF].

2015 San Bernardino terrorist attacks, when Apple refused to unlock the shooter's iPhone.[16] In a defining moment for the company, Apple's CEO, Tim Cook, wrote an open letter arguing that the United States' demands threatened the security of Apple's customers globally and that unlocking the shooter's iPhone would have significant implications beyond the San Bernardino attack.[17] Moreover, Apple stated, "the only way to guarantee that such a powerful tool isn't abused and doesn't fall into the wrong hands is to never create it."[18]

It is imperative that stakeholders pay close attention to the technology behind Apple's anti-CSAM tactics, since in Mr. Cook's words:

> what you build and what you create define[s] who you are. . . . And there are few areas where this is more important than privacy. . . . Too many seem to think that good intentions excuse away harmful outcomes.[19]

Unfortunately, Apple's leadership must navigate social, legal, and business interests without a straightforward solution.

C. Apple's iOS15 Anti-CSAM Updates and Encryption

NeuralHash, the safety feature that Apple announced in 2021 and later cancelled in December of 2022, works by creating unique identifiers (hash values) for users' photos that are stored on iPhone devices and are uploaded to one's iCloud Photo library.[20] These unique hash values are automatically compared against the hash values assigned to known CSAM that is kept in a centralized repository controlled by the National Center for Missing and Exploited Children (NCMEC) for CSAM detection purposes.[21] Hash value

[16] Alina Selyukh, *A Year After San Bernardino and Apple-FBI, Where Are We on Encryption?*, NPR (Dec. 3, 2016, 1:00 PM), https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption [https://perma.cc/U28M-SSBH].

[17] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/Q8GT-6627].

[18] *Answers to Your Questions About Apple and Security*, APPLE, https://www.apple.com/customer-letter/answers/ (last visited July 8, 2023) [https://perma.cc/YW2R-KB72].

[19] Tim Cook, *2019 Commencement Address by Apple CEO Tim Cook*, STAN. NEWS (June 16, 2019), https://news.stanford.edu/2019/06/16/remarks-tim-cook-2019-stanford-commencement/ [https://perma.cc/5MWH-DXZ6].

[20] *See Security Threat Model Review of Apple's Child Safety Features*, APPLE 5–11 (Aug. 2021), https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf [https://perma.cc/N6CF-BRXV].

[21] *Id.* at 6.

matching is a common practice; Apple's process is unique because its matching partially occurs on users' devices (client-side).[22] To clarify, all that is loaded onto users' devices are the numerical hash values assigned by NCMEC, not the CSAM itself.[23]

Encryption is a technique used to secure communications between a sender and receiver by converting plaintext into ciphertext message.[24] Businesses, militaries, governments, and individuals *all* use encryption to secure their data.[25] Apple uses encryption to safeguard their users' data, and Apple has stated that compromising their encryption would undermine its protections.[26] To Apple, encryption is a high priority because it "put[s customer] data out of [its] own reach, because [Apple] believe[s] the contents of your iPhone are none of [Apple's] business."[27] Apple's concerns about encryption were also the flashpoint in its fight with the United States Government in the San Bernadino investigation.

The term "hashing" is not synonymous with encryption; these techniques may be used together, or independently, to help safeguard information. However, they differ in important respects.[28] With encryption, the idea is that one party passes along information to a second party who then uses that information—known as a "key"—to decipher the otherwise encrypted contents of a message.[29] Hashing, on the other hand, involves an outside system administrator validating the authenticity of data post-transmission and determining whether it has been altered.[30] A deciphering key to view the original content of hashed data does not exist for parties

[22] APPLE, CSAM DETECTION: TECHNICAL SUMMARY 6 (2021), https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf [https://perma.cc/9H48-N2KJ] [hereinafter TECHNICAL SUMMARY]; *see* APPLE, EXPANDED PROTECTIONS FOR CHILDREN (2021), https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Technology_Summary.pdf [https://perma.cc/B6DK-BR2F] [hereinafter EXPANDED PROTECTIONS TECHNOLOGY].

[23] APPLE, EXPANDED PROTECTIONS FOR CHILDREN: FREQUENTLY ASKED QUESTIONS 4 (2021), https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf [https://perma.cc/5JML-C4ZM] [hereinafter FAQ]; TECHNICAL SUMMARY, *supra* note 22, at 6.

[24] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 714 (1995).

[25] *Id.* at 718.

[26] Cook, *supra* note 17.

[27] *Id.*

[28] *Encryption & Hashing: Simple Definitions*, OKTA, https://www.okta.com/identity-101/hashing-vs-encryption/ (last vistied July 29, 2023) [https://perma.cc/P4SZ-UA9N].

[29] *Id.*

[30] *Id.*

apart from the receiver and sender of the encrypted information.[31] Further, file-hashing functions create unique hash-value without comparing files' contents and any alterations to that data automatically generates a new hash-value.[32] Image-hashing functions enable comparisons between images that have been altered, but this technique intentionally allows for matches between altered images.[33]

Perceptual hashing as a technique is content agnostic.[34] Apple maintains that hash values, apart from those corresponding to the NCMEC database, cannot be added to its system.[35] Apple's policy in this respect is voluntary; it does not foreclose the company from modifying or expanding the application of the NeuralHash infrastructure beyond known-CSAM detection purposes in the future.

Many online providers, including Cloudflare, Gmail, Twitter, Facebook, and Microsoft, scan for CSAM in the cloud.[36] NeuralHash is different from other CSAM detection algorithms because it runs on users' physical devices *before* the images are uploaded onto iCloud Photos.[37] The iCloud user in this scenario must opt in to using iCloud Photos, otherwise the NeuralHash program will not run.[38] NeuralHash's cryptographic technology is powered by private set interaction (PSI) that looks for CSAM material without alerting the user and assigns that image a "safety voucher" before it uploads onto iCloud Photo.[39] Then, Apple runs a "threshold matching"[40] program on the images on iCloud, which prevents the system from scanning the safety vouchers associated with the uploaded images unless the total number of matches exceeds a certain numerical threshold.[41] According to Apple, if a user's image does not match against the known CSAM hash list, nothing about that image is learned.[42] Apple uses this threshold process because doing

[31] *See* Brief for Elec. Priv. Info. Ctr. as Amicus Curiae Supporting Defendant, United States v. Wilson, 13 F.4th 961 (2021) (No. 18-50440), https://epic.org/wp-content/uploads/amicus/algorithmic-transparency/wilson/EPIC-Amicus-Letter-People-v-Wilson-Filestamped.pdf [https://perma.cc/R3PS-GFJM].

[32] *Id.*

[33] *Id.*

[34] U.K. OFF. COMMC'NS, OVERVIEW OF PERCEPTUAL HASHING TECHNOLOGY 6 (2022), https://www.ofcom.org.uk/__data/assets/pdf_file/0036/247977/Perceptual-hashing-technology.pdf [https://perma.cc/MG5M-JYGF].

[35] *See* EXPANDED PROTECTIONS TECHNOLOGY, *supra* note 23, at 5–6.

[36] Callas, *supra* note 6.

[37] TECHNICAL SUMMARY, *supra* note 22, at 4.

[38] FAQ, *supra* note 23, at 2–4.

[39] APPLE, *supra* note 20, at 5.

[40] *Id.* at 6–7.

[41] *Id.* at 5.

[42] TECHNICAL SUMMARY, *supra* note 22, at 3.

so results in "an extremely low (1 in 1 trillion) probability of incorrectly flagging a given account."[43] Once that threshold is triggered, Apple will decrypt the corresponding safety voucher linked to flagged material, "allow[ing] Apple servers to access a visual derivative—such as a low-resolution version—of each matching image."[44] Apple's human reviewers then examine these visual derivatives to "confirm that they are CSAM material" and refer that user account to NCMEC.[45] Even though the probability of error in NeuralHash is low, errors may still occur. Approximately one month after Apple's announcement of NeuralHash, one individual published code demonstrating that he reverse-engineered an earlier version of NeuralHash to generate a "hash collision," where two entirely different pictures corresponded to the same hash value identifier.[46] Hash collisions present a systemic risk to cryptographic systems that rely on unique identifiers for their encryption. In this context, a hash collision also risks mislabeling content as CSAM to innocent users' peril.

The second feature Apple announced is its communication safety update in the Messages app for minors whose accounts are opted-in to the iCloud's Family Account feature.[47] According to Apple's public-facing documentation published in August of 2021 (which is still accessible online as of this writing), Apple scans communications transmitted within the Messages app for the presence of sexually explicit imagery and, if found, will send an alert to both the minor and their parents.[48] This feature uses an on-device machine learning classifier that sends two warnings to a Child Account user: first, asking if they wish to proceed, and second, informing them that an alert will also be sent to an associated parental account holder should they proceed.[49] For users between the ages of thirteen and seventeen, the minor is warned about the content and asked "if they wish to view or share a sexually explicit image"; however, their parents are not notified.[50] As of this writing, an undated

[43] *Id.* at 4.

[44] APPLE, *supra* note 20, at 5.

[45] *Id.* at 6.

[46] *See* Zack Whittaker, *Apple's CSAM Detection Tech Is Under Fire—Again*, TECHCRUNCH (Aug. 18, 2021, 12:28 PM), https://techcrunch.com/2021/08/18/apples-csam-detection-tech-is-under-fire-again/ [https://perma.cc/CY7X-2AHQ]; Joseph Cox et al., *Apple Defends Its Anti-Child Abuse Imagery Tech After Claims of 'Hash Collisions,'* VICE (Aug. 18, 2021, 11:38 AM), https://www.vice.com/en/article/wx5yzq/apple-defends-its-anti-child-abuse-imagery-tech-after-claims-of-hash-collisions [https://perma.cc/4XBM-DC6F].

[47] *See* FAQ, *supra* note 23, at 5.

[48] *Id.*

[49] *Id.*

[50] FAQ*, supra* note 23, at 3.

statement on Apple's website contradicts its August 2021 documentation, stating that "no notifications are sent to the parents or anyone else."[51]

Apple has not published information about how its on-device machine learning classifier for the Messages app works. Rather, Apple only states that "[t]he machine learning classifier used for this feature ships as part of the signed operating system . . . This claim is subject to code inspection by security researchers like all other iOS device-side security claims."[52] Also, Apple claims that this feature: (1) "cannot be enabled for an adult account, even with physical access to the device[,]"[53] and (2) it "does not reveal information to Apple[,] . . . does not disclose the communications of the users, the actions of the child, or the notifications to the parents[, and] does not compare images to any database, such as a database of CSAM material. It never generates any reports for Apple or law enforcement."[54]

Apple's initial announcement was met with concern from cryptographers[55] as well as prominent privacy-focused organizations who labeled these features as a "backdoor" to Apple's encryption.[56] Leading technologists also argued that client-side scanning for targeted content renders end-to-end encryption moot, and classified client-side scanning as indiscriminate bulk surveillance by another name.[57] The Electronic Frontier Foundation (EFF) and the Center for Democracy & Technology (CDT) both campaigned against NeuralHash's release, arguing that it is impossible to build a client-side scanning system that is only capable of detecting CSAM.[58] These critics pointed to the underlying content-neutrality of the NeuralHash algorithm as evidence that it could potentially be deployed

[51] *Child Safety*, APPLE, https://www.apple.com/child-safety/ [https://perma.cc/SXJ7-68D8].

[52] APPLE, *supra* note 20, at 4.

[53] *Id.* at 3.

[54] *Id.*

[55] *See* Jack Nicas, *Apple's iPhones Will Include New Tools to Flag Child Sexual Abuse*, N.Y. TIMES (Oct. 14, 2021), https://www.nytimes.com/2021/08/05/technology/apple-iphones-privacy.html [https://perma.cc/86GW-3MEN].

[56] *See* Cook, *supra* note 17; 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://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life [https://perma.cc/UZ5E-E3MN].

[57] Abelson et. al, *Bugs in Our Pockets: The Risks of Client-Side Scanning*, ARXIV 1, 2 (Oct. 14, 2021), https://arxiv.org/pdf/2110.07450.pdf [https://perma.cc/CS3A-6PNG].

[58] *See* McKinney & Portnoy, *supra* note 56; Emma Llansó, *What Could Go Wrong? Apple's Misguided Plans to Gut End-to-End Encryption*, CTR. FOR DEMOCRACY & TECH. (Aug. 11, 2021), https://cdt.org/insights/what-could-go-wrong-apples-misguided-plans-to-gut-end-to-end-encryption/ [https://perma.cc/3EAX-4DP5].

for different ends.[59] Their concern was that if Apple alters its machine learning parameters to flag different content, then any user account can be put at risk, which is not a mere "slippery slope [but rather] a fully built system just waiting for external pressure to make the slightest change."[60] In other words, even a "thoroughly documented, carefully thought-out, and narrowly-scoped [sic] backdoor [which] is still a backdoor."[61] Apple representatives contested this characterization of their safety features, arguing that their rollout "doesn't change Apple's [commitment to encryption] one iota. The device is still encrypted, we still don't hold the key, and the system is designed to function on on-device data."[62] Activists' scrutiny of Apple's announcement is a stark reminder that encryption is only a tool, not a virtual guarantee of privacy rights.

When Apple's Director of User Privacy, Mr. Erik Neuenschwander, was asked about this controversy, he stated that "[i]f you're storing a collection of CSAM material, yes, this is bad for you . . . [b]ut for the rest of you this is no different."[63] Although this remark may be well-intended, it minimizes serious concerns about "function creep"[64] from knowledgeable stakeholders, including criticism from within Apple.[65] This statement invokes the familiar notion that individuals should welcome surveillance infrastructure if they "have nothing to hide," and it ignores that pervasive surveillance infrastructure can be problematic in its own right. Furthermore, this notion insidiously equates support for pervasive surveillance infrastructure with being a law-abiding citizen.

[59] McKinney & Portnoy, *supra* note 56.

[60] *Id.*

[61] *Id.*

[62] Panzarino, *supra* note 2.

[63] Nicas, *supra* note 55.

[64] *See generally* Bert-Jaap Koop, *The Concept of Function Creep*, 13 L., INNOVATION & TECH. 29, 35 (2021).

[65] Joseph Menn & Julia Love, *Exclusive: Apple's Child Protection Features Spark Concern Within Its Own Ranks -Sources*, REUTERS (Aug. 12, 2021, 7:26 PM), https://www.reuters.com/technology/exclusive-apples-child-protection-features-spark-concern-within-its-own-ranks-2021-08-12/ [https://perma.cc/5M8Z-SZ3E].

If history has taught us anything, it's that even the most stalwart advocates of encryption and privacy are susceptible to business and political pressures.[66] Privacy activists' concern over Apple's decisions are not without historical basis in this regard.[67] Apple has compromised its commitment to privacy in countries like China, where it continues to store users' iCloud data on state-run telecom servers.[68] According to the New York Times, "Apple's compromises have made it nearly impossible for the company to stop the Chinese Government from gaining access to the emails, photos, documents, contacts and locations of millions of Chinese residents."[69] Apple houses customer data on these state-run servers to comply with a Chinese cybersecurity law, enacted in 2017, requiring all personal information collected in China to remain within China.[70] Apple initially said that it would hold onto the encryption keys to protect customer data despite this law; yet, those encryption keys were "headed to China" only eight months after this law came into effect.[71]

Even if the public were fully confident in Apple's assurances about its proposed safety features, Apple's choice to expand or narrow the scope of its surveillance tools amounts to a business decision.[72] Despite its best laid plans, it is feasible that Apple would compromise its purported values to appease government stakeholders globally.[73]

[66] *See, e.g.*, Amie Stepanovich & Michael Karanicolas, *Why an Encryption Backdoor for Just the "Good Guys" Won't Work*, JUST SEC. (Mar. 2, 2018), https://www.justsecurity.org/53316/criminalize-security-criminals-secure/ [https://perma.cc/YMG3-8LJH].

[67] *See, e.g.*, Nick Statt, *Apple's iCloud Partner in China Will Store User Data on Servers of State-Run Telecom*, VERGE (July 18, 2018, 12:37 PM), https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security [https://perma.cc/57WM-MHNX]; Jack Nicas et al., *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (June 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html [https://perma.cc/9LE9-6JP8].

[68] Statt, *supra* note 67.

[69] Nicas et al., *supra* note 67.

[70] *Id.*; *see* Paul Mozur et al., *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html [https://perma.cc/7U5U-M5NJ].

[71] Nicas et al., *supra* note 67.

[72] *See* Paul Rosenzweig, *The Apple Client-Side Scanning System*, LAWFARE BLOG (Aug. 24, 2021, 8:01 AM), https://www.lawfareblog.com/apple-client-side-scanning-system [https://perma.cc/RT3P-QPR8].

[73] *See* McKinney & Portnoy, *supra* note 5656; Llansó, *supra* note 58.

II. LEGAL BACKGROUND

A. The Fourth Amendment

A sense of privacy is central to the American identity, and it enables other rights enshrined in United States' founding documents (e.g., freedom of speech).[74] The Founding Fathers placed such a high premium on privacy that Justice Douglas later referred to it as a penumbral right impliedly found in the language of the United States Constitution.[75] The text of the Fourth Amendment enshrines "[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 [sic.] shall issue, but upon probable cause . . ."[76] According to the United States Supreme Court, the Fourth Amendment aims to secure the privacies of life against arbitrary power[77] and prevent "too permeating a police state."[78] Importantly, the Fourth Amendment only applies to government action; its protections do not apply to the voluntary conduct of private parties that do not act as government agents.[79] Its protective measures do not afford injunctive relief to the would-be subjects of government searches. The Fourth Amendment imposes a minimum standard for law enforcement to obtain probable cause warrant prior to searches and seizures,[80] yet this requirement is subject to certain exceptions.[81]

Fourth Amendment analysis generally involves a two-part test, asking: (1) "Was there a search by an applicable party?"; if so,

[74] *See Privacy & Free Expression*, BRENNAN CTR. FOR JUST., https://www.brennancenter.org/issues/protect-liberty-security/privacy-free-expression [https://perma.cc/WD59-YE52] ("The increase in government surveillance poses an unacceptable threat to privacy and freedom of speech."); Carly Nyst, *Two Sides of the Same Coin – The Right to Privacy and Freedom of Expression*, PRIV. INT'L (Oct. 7, 2013), https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression [https://perma.cc/AA5E-7H47] ("In this way, privacy and free expression are two sides of the same coin, each an essential prerequisite to the enjoyment of the other.").

[75] *See* Griswold v. Connecticut, 381 U.S. 479, 483–85 (1965) ("In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. . . . We have had many controversies over these penumbral rights of 'privacy and repose.'").

[76] U.S. CONST. amend. IV.

[77] Carpenter v. United States, 138 U.S. 2206, 2214 (2018) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

[78] *Id.* (citing United States v. Di Re, 332 U.S. 581, 595 (1948)).

[79] United States v. Jacobsen, 466 U.S. 109, 113–14 (1984).

[80] *See id.* at 117–18.

[81] *See generally* Payton v. New York, 445 U.S. 573 (1980) (discussing the exigent circumstances exception to the warrant requirement).

(2) "Was the search reasonable?"[82] The Court's understanding of the Fourth Amendment has evolved over time to broaden or narrow its view on whether a search has occurred in a particular case or controversy, which is a central component of Fourth Amendment cases as applied to new technologies.[83]

B. A Property-Based Fourth Amendment

According to the Supreme Court, "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass."[84] At that time, the home was "the prototypical and hence most commonly litigated area of protected privacy—[where] there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy."[85] The famous case, *United States v. Olmstead*, represents the clearest example of property-based Fourth Amendment jurisprudence.[86]

In *Olmstead,* the defendant was convicted of bootlegging spirits in violation of the National Prohibition Act using evidence gathered from a wiretap device.[87] The Supreme Court held that the government tapping a phone line located outside of the defendant's home was not a "search" under the Fourth Amendment.[88] The *Olmstead* Court looked to various factors when employing historical and technological analogy in its analysis, explaining:

> *Ex parte* Jackson . . . offers an analogy to the interpretation of the Fourth Amendment in respect of wiretapping [sic]. But the analogy fails. The Fourth Amendment may have proper application to a sealed letter in the mail . . . . The amendment does not forbid what was done here. There was no searching. There was no seizure . . . . There was no entry of the houses or offices of the defendants.[89]

In his dissenting opinion, Justice Brandeis presciently invoked the immortal words of Chief Justice Marshall's opinion in *McCulloh v. Maryland*, writing:

[82] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[83] *See id.*; Olmstead v. United States, 277 U.S. 438, 479 (1928).

[84] Kyllo v. United States, 533 U.S. 27, 31 (2001).

[85] *Id.* at 34 (emphasis added).

[86] *See generally* Olmstead, 277 U.S. 438.

[87] *Id.* at 455.

[88] *Id.* at 466.

[89] *Id.* at 464.

> '[i]t is a Constitution [sic] we are expounding.' Since then[,] this court has repeatedly sustained the exercise of power by Congress, under various clauses of that instrument, over objects of which the fathers could not have dreamed.[90]

Justice Brandeis' foreboding reminder rings true to this day.

C. The Fourth Amendment Protects People, Not Property

In 1967, the Supreme Court deviated from its property-based Fourth Amendment jurisprudence toward a "people-based" understanding in the watershed case, *Katz v. United States*.[91] The facts of *Katz* involved the government wiretapping a public phonebooth, with a much different outcome than *Olmstead*.[92]

The *Katz* majority rejected the government's claim that law enforcement's actions did not implicate the Fourth Amendment, since it only applied to "constitutionally protected areas."[93] The Court's renunciation of *Olmstead* paved the way for a less literal interpretation of the Fourth Amendment. Another major contribution of *Katz* lies in Justice Harlan's concurrence, which, since introduced, has been referred to as the "*Katz* test." The test sets out a standard for a "reasonable expectation of privacy" (REP), which imposes "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.'"[94] Since then, the Court's Fourth Amendment analysis ceased being an exercise in physical line drawing exclusively. It evolved to also weigh the figurative bounds of individuals' reasonable expectations.

Staking the boundaries of individuals' REP is a controversial endeavor and there are at least two significant criticisms of the *Katz* test. The first criticism is that, in practice, individual judges decide whether one's expectation of privacy is "objectively reasonable"; yet, judges may not be the appropriate authority to make such pronouncements regarding privacy.[95] Judges, according to Justice Alito, "are apt to confuse their own expectations of privacy with

[90] *Id.* (Brandeis, J., dissenting) (citing McCulloch v. Maryland, 17 U.S. 316, 407 (1819)).

[91] Katz v. United States, 389 U.S. 347, 353 (1967).

[92] *Id.* at 348.

[93] *Id.* at 351.

[94] *Id.* at 361 (Harlan, J., concurring).

[95] *See* DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 299 (6th ed. 2018) ("Currently, judges decide whether a defendant has a reasonable expectation of privacy in a particular activity. Is this an appropriate question for judge to decide? Or should juries decide it? . . . Is it an empirical question about what most people in society would generally consider to be private?").

those of the hypothetical reasonable person to which the *Katz* test looks."[96] Second, the *Katz* test suffers from circular reasoning[97] in addition to what this paper identifies as the *Katz* test's "outside actor problem." Justice Kennedy described the *Katz* test's circularity as the Court "bas[ing] its decisions on society's expectations of privacy, [yet] society's expectations of privacy are in turn shaped by [the] Court's decisions."[98] That description, however, does not account for outside parties' intentional efforts to influence this process.

In addition to circular reasoning, outside actors' intentional acts are a confounding variable that influence an individual's subjective expectation of privacy (*Katz* prong one) as well as courts' decisions to see if the individual's belief is objectively reasonable (*Katz* prong two). Therefore, the *Katz* test is susceptible to exploitation by outside actors with a vested interest in curtailing the bounds of individuals' REP. The outside actor problem of the *Katz* test is significant because, over 60 percent of Americans reportedly believe "it is not possible to go through daily life without companies [or the government] collecting data about them" and over 80 percent of Americans feel "as if they have little control over data collected about them by companies and the government."[99] Therefore, judges' attempts at objectivity may simply legally affirm the socially-engineered salience of outside actors' invasive practices in deciding whether one's expectation of privacy is objectively reasonable.

D. *The Third-Party Doctrine*

The third-party doctrine emerged out of a series of cases concerning whether an individual maintains his or her REP in information provided to a third party.[100] The two canonical third-party doctrine cases are *United States v. Miller* and *Smith v. Maryland*.

In *Miller*, the Court held the defendant did not have a reasonable expectation of privacy in his bank deposit records, which were

[96] United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[97] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[98] Carpenter v. United States, 138 U.S. 2206, 2245 (2018) (Kennedy, J., dissenting).

[99] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/3Q58-4WB6].

[100] *See* Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012), https://www.law.uh.edu/faculty/eberman/security/The%20Data%20Question_%20Should%20the%20Third-Party%20Records%20Doctrine%20Be%20Revisited_.pdf [https://perma.cc/QC9J-5TSQ].

not his "private papers," because they were the bank's business records.[101] Therefore, he could "assert neither ownership nor possession [over those documents]."[102] The Supreme Court noted that the defendant had no reasonable expectation of privacy in his deposited bank checks because they were "negotiable instruments," as opposed to private communications with confidential content, which the defendant freely provided to the bank in the institution's "ordinary course of business."[103]

In *Smith*, the Court held that a telephone company installing a pen register did not qualify as a "search" under the Fourth Amendment.[104] The *Smith* Court proffered two justifications for its holding: (1) the telephone company installed a pen register on property that did not belong to the defendant and (2) the facts of *Smith* were distinguishable from *Katz* because the data collected was exclusively non-content data.[105] The Court reasoned that, when an individual dials a phone number, they knowingly convey that information to the service provider.[106] The *Smith* Court concluded that individuals inherently realize telephone companies possess the capability to legitimately record certain non-content information in order to maintain adequate "business records," and that telephone companies actually create such records of non-content.[107] Consequently, when the defendant in *Smith* conveyed the dialed numbers to the service provider, he assumed the risk of disclosure by a third party and did not have a reasonable expectation of privacy in the numbers dialed.[108]

In recent years, Justices have signaled a strong need to reconsider the third-party doctrine's future in the era of Big Data. Two cases, *U.S. v. Jones* and *Carpenter v. U.S.*, offer a limiting principle to the third-party doctrine.[109]

The Court in *Jones* held that the police conducted a "search" of the defendant's private property by attaching a GPS device to the undercarriage of the defendant's car.[110] The Court determined his

[101] United States v. Miller, 425 U.S. 435, 440 (1976).

[102] *Id.*

[103] *Id.* at 442.

[104] Smith v. Maryland, 442 U.S. 735, 746 (1979).

[105] *Id.* at 741.

[106] *Id.* at 743.

[107] *Id.* at 742.

[108] *Id.* at 744.

[109] *See* Orin Kerr, *Understanding the Supreme Court's Carpenter Decision,* LAWFARE BLOG (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/N983-S5DS].

[110] United States v. Jones, 565 U.S. 400, 404 (2012).

car was an "effect" within the meaning of the Fourth Amendment.[111] The Court also explained that an individual's REP is not the only measure for Fourth Amendment protections because "the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."[112] Furthermore, in her concurrence, Justice Sotomayor questioned the viability of the third party doctrine, highlighting:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . 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.[113]

Her concurrence offers potentially precedential guideposts for future legal battles on this subject.

In *Carpenter*, the Court declined to extend *Smith* and *Miller* to cell-site location information (CSLI) records—a continuous catalog of one's physical movements using cell phone towers, which provides wireless network connectivity for mobile devices.[114] Although wireless carriers collect CSLI for legitimate business purposes, the Court ruled that the contents of the information sought in *Smith* and *Miller* were too different in kind from CSLI and extending the third-party doctrine to CSLI would be expanding it to cover a distinct type of information not considered in earlier case law.[115]

E. The Private Search Doctrine

When defendants raise the Fourth Amendment in a CSAM context, the private search doctrine is relevant, as the Fourth Amendment only applies to private parties "acting as an agent of the Government [sic] or with the participation or knowledge of any governmental official."[116] Courts interpret the question of whether a private party acted as a government agent through the lens of

[111] *Id.*

[112] *Id.* at 409.

[113] *Id.* at 417–18 (Sotomayor, J., concurring).

[114] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[115] *Id.* at 2219.

[116] United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003) (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

common-law agency principles,[117] including if they provided the evidence to the government "on their own accord."[118] Notably, in *United States v. Ackerman*, then Tenth Circuit judge Neil Gorsuch held that NCMEC is a government entity.[119]

Courts are split over the application of the private search doctrine, based on their understandings of how specific anti-CSAM technologies work.[120] Per this doctrine, if a private party conducts a search, "the Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."[121] In turn, this doctrine has significant implications for Apple's CSAM-targeting features, and it raises questions about whether it would evaluate a search by NeuralHash differently than other anti-CSAM processes due to its client-side scanning component. In other words, does client-side scanning from NeuralHash reduce iPhone-users' REP in their devices more generally?

A recent controversy, involving both federal and state CSAM charges, illustrates courts' confusion about the applicability of this doctrine to modern CSAM-scanning technologies. The two cases involved Microsoft's PhotoDNA identifying CSAM in the same defendant's emails, which ultimately led to criminal charges. Wilson, the defendant, faced a series of federal and state charges and was tried in two separate cases, *U.S. v. Wilson* and *People v. Wilson*.[122] The Court of Appeals for the Ninth Circuit and the California Court of Appeal, respectively, reached opposite conclusions about Wilson's REP in his emails based on their different understandings of how the CSAM detection technology used works. As a result of their disagreement, one commentator observes, "two appellate courts with overlapping jurisdiction over the same search are in conflict with one another, which is highly unusual."[123] The Ninth Circuit also

[117] *Id.*

[118] United States v. Wilson, 13 F.4th 961, 967 (9th Cir. 2021) (citing Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971)).

[119] *See* United States v. Ackerman, 831 F.3d 1292, 1297 (10th Cir. 2016) ("Recent Supreme Court decisions fortify our conviction that NCMEC qualifies as a governmental entity."); *see also* MICHAEL A. FOSTER, CONG. RSCH. SERV., LSB10713, THE FOURTH AMENDMENT AND THE INTERNET: LEGAL LIMITS ON DIGITAL SEARCHES FOR CHILD SEXUAL ABUSE MATERIAL CSAM 3 (2022).

[120] *See* People v. Wilson, 56 Cal. App. 5th 128, 145 (2020); United States v. Wilson, 13 F.4th at 978–79.

[121] United States v. Jacobsen, 466 U.S. 109, 117 (1984).

[122] *See* Jennifer Lynch, *In U.S. v. Wilson the Ninth Circuit Reaffirms Fourth Amendment Protection for Electronic Communications*, ELEC. FRONTIER FOUND. (Sept. 28, 2021), https://www.eff.org/deeplinks/2021/09/us-v-wilson-ninth-circuit-reaffirms-fourth-amendment-protection-electronic [https://perma.cc/35LH-7JW9].

[123] *Id.*

expressly rejected the Fifth and Sixth Circuits' applications of the private search doctrine in their recent CSAM cases.[124]

The facts of Wilson's case are important for understanding why the Ninth Circuit and California Court of Appeal disagree. On June 4, 2015, Wilson sent CSAM through his email account, which Google's proprietary technology identified and subsequently reported through CyberTipline to NCMEC.[125] However, the CSAM at issue was never visually confirmed by a Google employee after the report was automatically generated.[126] Once NCMEC received the report, it appropriately forwarded it to the San Diego Internet Crimes Against Children Task Force (ICAC), where an agent visually inspected its contents.[127] The agent then applied for a warrant to search the defendant's email account, which was granted based on the agent's affidavit.[128] Then, the agent searched the defendant's account, where he discovered emails offering to pay for CSAM.[129]

In the federal case, *U.S. v. Wilson*, the Ninth Circuit held that the government's actions were not covered by the private search exception; therefore, the defendant maintained a REP in his emails under a traditional Fourth Amendment analysis.[130] Per the Court's analysis, ICAC's search violated the Fourth Amendment because: (1) it allowed the government to acquire evidence of wrongdoing beyond the scope of the Google's prior private search[131] and (2) the Google employee did not actually view the CSAM contained in the report—the ICAC agent's opening of the email attachments to view CSAM "exceed[ed] an earlier privacy intrusion."[132] The panel also alluded to Google's lack of transparency about employee training and how the company's algorithms created a limited evidentiary record that did not detail what the employee saw.[133] The record did indicate, however, that Google maintains a repository of hash values for detection purposes, rather than the actual CSAM.[134]

In *People v. Wilson*, the California Court of Appeal held that the agent's viewing of the CyberTipline report did not implicate the

[124] United States v. Wilson, 13 F.4th 961, 978–79 (9th Cir. 2021).
[125] *Id.* at 965.
[126] *See id.* at 965.
[127] *Id.*
[128] *Id.* at 965–66.
[129] United States v. Wilson, 13 F.4th 961, 966 (9th Cir. 2021).
[130] *See id.* at 971–72.
[131] *See id.*
[132] *Id.* at 972.
[133] *Id.* at 965.
[134] United States v. Wilson, 13 F.4th 961, 965 (9th Cir. 2021).

Fourth Amendment.[135] The California Court of Appeal reasoned that Google's scan with PhotoDNA had already frustrated Wilson's REP in his emails prior to ICAC's subsequent visual inspection—i.e. law enforcement's "search."[136] Instead, the inspection "merely enabled the government to confirm [what] Google already conveyed . . . [which] did not further infringe on Wilson's privacy, but rather guarded against the risk that Google's report was wrong."[137] Furthermore, the Court found that Google's processes "are properly viewed in their entirety as equivalent to a private search"[138] because its employees index CSAM with a "digital fingerprint" (the hash value) and its matching process only looks for previously identified CSAM.[139] In turn, the Court described having a Google employee's visual confirmation of the exact CSAM contained in a CyberTipline Report prior to the ICAC inspection as a "redundant step."[140] Thus, the Court found that fully-automated CSAM detection and reporting without employee confirmation fell within the scope of the private search exception and did not trigger a Fourth Amendment analysis.

F. The Electronic Communications Privacy Act of 1986 (ECPA)

The final body of law implicated by CSAM scanning technology is the Electronic Communications Privacy Act of 1986 (ECPA). Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, following the Supreme Court's decision in *Katz*.[141] "Since that time," according to Justice Alito, "electronic surveillance has been governed primarily, not by decisions of [the Supreme] Court, but by the statute, which authorizes and imposes detailed restrictions on electronic surveillance."[142] Then, in 1986, Congress enacted the ECPA, which is comprised of three different legislative acts governing electronic communications: a revised version of The Wiretap Act, The Stored Communications Act (SCA), and The Pen Register Act.[143]

[135] *See* People v. Wilson, 56 Cal. App. 5th 128, 145 (2020).

[136] *Id.* at 144–45.

[137] *Id.* at 145–46.

[138] *Id.* at 148.

[139] *Id.* at 149.

[140] People v. Wilson, 56 Cal. App. 5th 128, 148 (2020).

[141] Riley v. California, 573 U.S. 373, 408 (2014).

[142] *Id.*

[143] The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (including the Wiretap Act, 18 U.S.C. § 2510 et seq., the Stored Communications Act, 18 U.S.C. § 2701 et seq., and the Pen Register Act, 18 U.S.C. § 3121 et seq.).

The ECPA has been characterized by some courts as "famous (if not infamous) for lack of clarity."[144] Each component of the ECPA governs different forms of communications, including the corresponding levels of judicial supervision necessary for law enforcement to access them.[145] Unlike the Fourth Amendment, the ECPA applies to both private and state action. Importantly, in instances where law enforcement fails to follow the ECPA's proscribed procedural requirements, courts will revert to a Fourth Amendment REP analysis to determine the constitutionality of the search at issue.

The Wiretap Act[146] governs the intentional interceptions of wire and aural communications. Under the Wiretap Act, law enforcement must receive a "warrant-plus" requiring a judge to find (1) probable cause of a felony activity; (2) that alternatives to wiretapping will not suffice in gathering the sought-after information; and (3) the sought-after information will likely be obtained through the wiretap.[147] A warrant-plus may last for up to 30 days, may only be obtained by certain government officials, and must meet certain minimization requirements.[148] Thus, the Wiretap Act has a more rigorous evidentiary standard than a probable cause warrant as required under the Fourth Amendment. The Wiretap Act also includes exceptions to its general rule of prohibiting the intentional interception of aural communications by permitting electronic communications services' (ECS) interceptions executed in their ordinary course of business.[149] However, most courts narrowly interpret this exemption and require a demonstrable "nexus between the need to engage in the alleged interception and the user's, subscriber's, or ECS' ability to provide the underlying service or good."[150]

The SCA applies to electronic communications at rest or held in storage, including temporary and backup storage.[151] When applied, the SCA's procedural oversight requirements differ based on

[144] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994).

[145] *See* CHARLES DOYLE, CONG. RSCH. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2012).

[146] 18 U.S.C. § 2510 et seq.

[147] 18 U.S.C. § 2518.

[148] *Id.*

[149] 18 U.S.C. § 2510(5)(a)(i).

[150] Eric Bosset, *Key Issues in Electronic Communications Privacy Act (ECPA) Litigation*, THOMSON REUTERS PRAC. NOTES, W-023-5320.

[151] United States v. Warshak, 631 F.3d 266, 282–83 (6th Cir. 2010).

the length of time the communication itself has been held in storage.[152] If it has been stored for 180 days or less, a probable cause warrant is required.[153] Beyond the 180 day mark, the government may use either an administrative, grand jury, trial subpoena, or court order (with a sufficient demonstration of its relevance to an ongoing investigation).[154] In the SCA, ECSs and remote computing service providers (RCSPs) may be liable for knowingly sharing stored communications.[155] However, Section 2702 authorizes the voluntary disclosure of customer communications and customer records by Electronic Communications Providers (ECP) to NCMEC, law enforcement agencies, and other government entities.[156] One exception to prohibited disclosure of communications is if it is "necessarily incident to the rendition of the service or to the protection of the rights of property of the provider of that service."[157] Additionally, an ECP may voluntarily disclose customer communications and customer records to NCMEC while reporting CSAM in accordance with 18 U.S.C. Section 2258A ("Assessments in Child Pornography Cases").[158]

G. *The Disharmony Between the ECPA and the Fourth Amendment*

The ECPA governs an astronomical number of interactions in society,[159] and, as previously discussed, permits law enforcement to satisfy a lower evidentiary standard for some types of communications and a higher standard for others. Importantly, however, recent judicial interpretations of the Fourth Amendment as applied to cell phone information indicate a developing conflict between the ECPA's tiered framework and the Fourth Amendment more broadly. The Supreme Court's decisions in both *Riley* and *Carpenter*, along with the Sixth Circuit's decision in *U.S. v. Warshak*, further illustrate the growing divide between the two sources of law.

In both *Riley* and *Carpenter*, the Supreme Court refused to mechanically follow either Fourth Amendment doctrine or the ECPA

[152] *See* Bosset, *supra* note 150.

[153] 18 U.S.C. § 2703(a).

[154] *See* 18 U.S.C. § 2703(b).

[155] *See* 18 U.S.C. § 2702(a)(2), 2707(a).

[156] 18 U.S.C. §§ 2702(b)(6), 2702(b)(7), 2702(b)(8), 2702(c)(4), 2702(c)(5).

[157] 18 U.S.C. § 2702(b)(5).

[158] 18 U.S.C. §§ 2702(b)(6), -(c)(5).

[159] *See, e.g.*, Riley v. California, 573 U.S. 373, 395 (2014) ("[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

respectively to preserve the Fourth Amendment's broadest command.[160] The Court's actions in these cases beg the question: Why permit lesser judicial oversight protections under the SCA and potentially allow the government to obtain information that would otherwise require a probable cause warrant?

In *Riley*, the Supreme Court held that the police implicated the Fourth Amendment after searching an arrestee's cell phone without a warrant.[161] The Court distinguished cell phones from other personal effects that could reasonably be on one's person at the time of an arrest.[162] The Court also acknowledged that cell phone data contains a further level of complexity because local phone data is entangled with cloud storage which:

> [c]omplicat[es] the scope of the privacy interests at stake, [because] the data a user views on many modern cell phones may not in fact be stored on the device itself. . . . Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.[163]

While the location of data makes little difference in the user experience, as a procedural matter, cloud-hosted data would not otherwise be accessible to an arresting officer, but for the novel capabilities of cell phones.[164] Moreover, an officer who searches an arrestee's cell phone would ordinarily have no way to determine whether the information they are viewing on a device is cloud-hosted, stored on the device, or both.[165] Instead of allowing law enforcement to retroactively audit the cell phone data on the subject-device, the Court drew a bright-line: "[t]he answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[166]

In *Carpenter*, the Court noted that cell-site location information (CSLI) "does not fit neatly under existing precedents."[167] Even though the Court limited its holding to CSLI alone, it sidestepped the ECPA's rigid treatment of different data types to preserve constitutional minimums.[168] The government obtained the

[160] *See e.g.*, *id.*; Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[161] Riley, 573 U.S. at 401.

[162] *Id.* at 393.

[163] *Id.* at 397.

[164] *Id.* at 396–97.

[165] *Id.* at 397.

[166] Riley v. California, 573 U.S. 373, 403 (2014).

[167] Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018).

[168] *See id.* at 2220.

defendant's CSLI using a court order pursuant to the SCA.[169] Writing for the majority, Chief Justice Roberts determined that the SCA's judicial oversight was insufficient for CSLI, and that "before compelling a wireless carrier to turn over a subscriber's CSLI, the Government [sic] obligation is a familiar one—get a warrant."[170] To paraphrase, in choosing to evaluate the unique properties of CSLI the Court disregarded the SCA.

Relatedly, in some instances, ECPA places a higher standard than a probable cause warrant; however, the Constitutional minimums guaranteed by the Fourth Amendment are not upheld across ECPA's components (the Wiretap Act, the SCA, and the Pen Register Act). For example, in *U.S. v. Warshak*, the Sixth Circuit held that the defendant maintained a reasonable expectation of privacy in the content of his emails and that the government violated his Fourth Amendment rights by forcing his internet service provider to provide those emails to the government without a probable cause warrant.[171] Further, the Court held that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[172]

The *Warshak* Court applied the *Katz* test and held that the defendant had a subjective expectation of privacy (step one) in his emails due to the "sensitive and sometimes damning substance" of his communications.[173] Next, the Court held that the defendant's subjective belief was objectively reasonable (step two) because internet-based communication has increased in its societal importance whereas physical letters and telephone calls have comparatively decreased.[174] The *Warshak* Court further justified its holding on two "bedrock principles" (1) that the passing of information through a communications service is significant to the Fourth Amendment[175] and (2) "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[176] Finally, the Court compared the facts of *Katz* (wiretapping a telephone line) and *Ex parte Jackson* (viewing the contents of a physical letter) to the defendant's emails and reasoned, "it would defy common sense to afford email

[169] *Id.* at 2221.

[170] *Id.*

[171] *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).

[172] *Id.* at 288.

[173] *Id.* at 284.

[174] *Id.*

[175] *Id.* at 285.

[176] United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

lesser Fourth Amendment protection."[177] The Court observed that, while it is theoretically possible for a third-party's subscriber agreement (user agreement) to potentially defeat an individual's expectation of privacy in the contents of their communications, it is "doubt[ful] that will be the case in most situations" and that a third-party's "*right* of access" or that "the mere *ability* . . . to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[178]

In sum, considering new technological developments, it appears that some courts question the constitutional sufficiency of the SCA's judicial oversight measures (or lack thereof) for certain data.

III. THE SCOPE OF IPHONE DEVICE HOLDERS' OWNERSHIP INTERESTS

A. *Why Device Ownership Is Relevant*

While property ownership is not entirely decoupled from Fourth Amendment jurisprudence,[179] colloquial understandings of what it means to "own" something does not necessarily comport with "property" that is subject to lengthy terms of service and use by the seller. Smartphone owners, for example, likely do not realize that a complex property structure governs various aspects of their interest in their device apart from the physical hardware. Some commentators in the technology community believe that Apple's mistake throughout this saga was that it "betray[ed] the fulcrum of user control: being able to trust that your device is truly yours."[180] This is an especially important consideration, seeing as subjective expectations are only one prong of the two-part *Katz* test. An individual's subjective expectation of privacy must also be objectively reasonable in the eyes of the court. The ECPA framework, moreover, accounts for property considerations in its exceptions for electronic communications delivered through and stored on service providers' technology infrastructure, which end users do not own.

Moreover, one's personal assumptions regarding property ownership do not displace the legal terms and conditions of the iOS and iPad OS Software License Agreement ("User Agreement"). Apple possesses the ability to perform remote software security updates, application performance monitoring functions, and collect user data

[177] *Id.* at 285–86.

[178] *Id.* at 286–88 (emphasis in original).

[179] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

[180] Ben Thompson, *Apple's Mistake*, STRATECHERY (Aug. 9, 2021), https://stratechery.com/2021/apples-mistake/ [https://perma.cc/8UTQ-P23J].

from iPhone devices in line with its governing documents (e.g., User Agreement, and the Apple Privacy Policy).

B. The Terms of Apple's iOS Software License Agreement (the "User Agreement")

The average iPhone user may, understandably, believe they "own their phone," without giving much thought to the anatomy of their smartphone, its hardware and software, and their corresponding ownership interests in each component.[181] The iOS15 system is set to incorporate the NeuralHash program as well as the communication safety features in Apple's Messages application.[182] Users of iOS15 are bound by the terms set forth in the Apple iOS AND iPadOS Software License Agreement ("User Agreement") that states, in bold, capital letters "if you do not agree to the terms of this license, do not use the device or download the software update."[183] Ostensibly, this presents consumers with a Hobson's choice: agree to Apple's terms or don't use Apple products. This choice may sound reasonable; however, Apple's iOS accounted for 56.74 percent of the U.S. mobile operating system market share in 2022 and Google's Android OS accounted for 42.94 percent.[184] Beyond Apple's arguably dominant market position, consumers may not have any meaningful choice because other providers may have equally burdensome terms in their terms of service. Another important provision in Apple's User Agreement is that users may opt to have software updates automatically installed on their devices, but this is not the default setting.[185] According to this contract, users do not own the software on their iPhone.[186] Rather, they are "granted a limited non-exclusive license to use the Apple Software on a single Apple-branded Device."[187] When using an Apple device,

[181] *See* Rob Pegoraro, *Who Really Owns Your iPhone? It May Not Be You*, YAHOO! FIN. (Sept. 18, 2015), https://finance.yahoo.com/news/who-really-owns-your-iphone-it-may-not-be-you-129321095449.html [https://perma.cc/4KBT-ZALE].

[182] *See* Jon Porter, *Apple Scrubs Controversial CSAM Detection Feature from Webpage but Says Plans Haven't Changed*, VERGE (Dec. 15, 2021, 11:56 AM), https://www.theverge.com/2021/12/15/22837631/apple-csam-detection-child-safety-feature-webpage-removal-delay [https://perma.cc/8XW8-2MF5].

[183] APPLE, APPLE IOS AND IPADOS SOFTWARE LICENSE AGREEMENT 1, https://www.apple.com/legal/sla/docs/iOS15_iPadOS15.pdf [https://perma.cc/R6CG-LJVG].

[184] *Mobile Operating System Market Share United States of America*, STAT COUNTER, https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/#monthly-202201-202212-bar [https://perma.cc/6ZFB-U8YU].

[185] APPLE, *supra* note 183, at 3.

[186] *Id.* at 2.

[187] *Id.*

customers automatically consent to the terms and conditions of using Apple's software license.[188] Although the physical Apple device may be the tangible property of a user, the individual does not have permission to modify the Apple software in any way.[189] Finally, the Agreement states that Apple's collection and use of users' personal information is governed by the Apple Privacy Policy.[190]

C. Apple's Privacy Policy

Apple's Privacy Policy states, Apple "believe[s] strongly in fundamental privacy rights" and, for that reason, Apple "treat[s] any data that relates to an identified or identifiable individual or that is linked or linkable to [Apple's customers] by Apple as 'personal data,' no matter where that person lives."[191] Per company policy, Apple "strive[s] to collect only the personal data that [it] needs."[192] Apple uses personal data "only for so long as necessary to fulfill the purposes for which it was collected . . . or as required by law."[193] Furthermore, Apple maintains that it reserves the right to process users' data when "it is in [Apple's] or others' legitimate interests, taking into consideration [users'] interests, rights, and expectations."[194] Significantly, Apple also retains the right to alter the terms of its privacy policy.[195]

IV. A NEW FRAMEWORK

A. Applying These Sources of Law to the iPhone

As discussed earlier, communication in transit is subject to the Wiretap Act; however, once in storage, that data is governed by the SCA.[196] Naturally, the SCA has carveouts for ECPs' cooperation with law enforcement, and for turning over CSAM to NCMEC.[197]

Under the Fourth Amendment, the Supreme Court has stated that law enforcement's search of a smartphone requires them to first obtain a warrant.[198] Even so, smartphone data routinely

[188] *Id.* at 1.

[189] *Id.* at 2.

[190] *Id.* at 12.

[191] APPLE, APPLE PRIVACY POLICY 2 (2022), https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf [https://perma.cc/E3FS-2AVV].

[192] *Id.* at 3.

[193] *Id.* at 5.

[194] *Id.*

[195] *Id.* at 5.

[196] *See* discussion *supra* Part II.

[197] *See id.*

[198] *See* Riley v. California, 573 U.S. 373, 401 (2014).

comes into the government's possession due to the third-party doctrine (which is untenable in the digital age) as well as the private search doctrine.

Turning to Apple's controversial safety features, when law-abiding citizens opt in to using iCloud Photo, NeuralHash would have performed its hash value matching directly on these users' devices.[199] This raises the question: What affect does client-side scanning have on an individual's REP? In other words, what is an objectively reasonable expectation of privacy in one's iPhone in a post-NeuralHash world? Client-side scanning may well invite further opportunities for the judiciary to inconsistently apply the private search doctrine. As previously discussed, the *Wilson* Courts came to opposing conclusions about server-side scanning,[200] and the Supreme Court declined to grant certiorari, arguably meaning their debate over warrantless private searches remains unresolved.[201]

Given these rapidly evolving technological capabilities, society needs another privacy-preserving mechanism. To preserve the spirit of the Fourth Amendment in the digital age, the Supreme Court should consider giving the same level of protection to encrypted smartphone communications as it does to the physical walls of one's home. Such a view takes root in the original property-based conception of the Fourth Amendment and would help resolve the circular reasoning and third-party problems in the *Katz* test.

B. Reasons Why This Framework Works

According to Chief Justice Roberts' majority opinion in *Riley*, modern cell phones are "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[202] Looking ahead, it is fair to assume that the ECPA's outsized relevance in our society relative to the Fourth Amendment will only continue to increase based on industry projections about the growth of interconnected

[199] *See* discussion *supra* Part I.

[200] *See* discussion *supra* Part II.

[201] Andrea Vittorio, *Supreme Court Declines to Review Google-Flagged Child Porn Case*, BLOOMBERG L. (Jan. 10, 2022, 7:41 AM), https://news.bloomberglaw.com/litigation/supreme-court-declines-to-review-google-flagged-child-porn-case [https://perma.cc/JM9G-5FU3].

[202] Riley, 573 U.S. at 385.

devices,[203] resulting in the integration of the digital and physical worlds.[204]

This framework is sound for several reasons. It utilizes comparative analysis of different technologies in a search context, which is a staple of the Supreme Court's Fourth Amendment jurisprudence. Indeed, the Supreme Court previously likened the information kept on cell phones to the contents of one's home in *Riley*, stating "a phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[205] Cell phones house our deepest intimacies and provide extremely detailed views into our private lives.

Walls are a barrier between oneself and the outside world, creating the necessary space for occupants to safeguard the intimate details of their lives—i.e., their "papers or effects"—which are protected from unreasonable searched and seizures by the United States Government.[206] In this sense, encryption serves a similar function and could be viewed as such in a search context. Much like a locked door, a wall, or gate, encryption uses cryptographic characteristics (signing and encryption) to receive an input (the key and message) and generate an output and provide access (ciphertext), ultimately serving the end of protecting information.[207]

This property-inspired metaphor aligns with longstanding Fourth Amendment doctrine. As explained in *Jones*, the *Katz* test is not a substitute for the common-law trespassory test of the *Olmstead* era.[208] In addition to considerations about one's reasonable expectations of privacy, "the Fourth Amendment draws 'a firm line at the entrance to the house'. . . . [which] must be not only firm but also bright. This requires clear specification of those methods of surveillance that require a warrant."[209] Such an understanding

[203] *Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030, with Forecasts from 2022 to 2030*, STATISTA (Oct. 19, 2021), https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [https://perma.cc/4ANJ-ECFZ].

[204] MAJORITY STAFF OF H. COMM. ON HOMELAND SEC., 114TH CONG., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE 7 (Comm. Print 2016).

[205] Riley, 573 U.S. at 396–97.

[206] U.S. CONST. amend. IV.

[207] *See* SENY KAMARA ET AL., CTR. FOR DEMOCRACY & TECH., OUTSIDE LOOKING IN: APPROACHES TO CONTENT MODERATION IN END-TO-END ENCRYPTED SYSTEMS 13 (Aug. 12, 2021), https://cdt.org/wp-content/uploads/2021/08/CDT-Outside-Looking-In-Approaches-to-Content-Moderation-in-End-to-End-Encrypted-Systems-updated-20220113.pdf [https://perma.cc/W99X-6DWM].

[208] *See* United States v. Jones, 565 U.S. 400, 409 (2012).

[209] Kyllo v. United States, 533 U.S. 27, 40 (2001) (quoting Payton v. New York, 445 U.S. 573, 590 (1979)).

could also help mitigate the effect of the *Katz* test's circular reasoning and outside actor problems in situations where the *Katz* test falls short. This framework may be considered a supplement to, rather than a replacement of, the *Katz* reasonable expectation of privacy test. [210]

Moreover, if the United States Government were to use non-publicly available software to break a smartphone's encryption, this framework would provide an effective judicial backstop. In *Katz*, the Supreme Court held that "the Fourth Amendment protected [the defendant] from the warrantless eavesdropping because he 'justifiably relied' upon the privacy of the telephone booth."[211] Similarly, Apple represents that its encryption practices are a privacy-preserving tool that its users may rely on.[212] Yet, in light of the ECPA framework and the private search doctrine, it remains possible that this reasoning alone would not withstand judicial scrutiny. If the Supreme Court were to recognize encryption as akin to the walls of one's home in a search context, then the means used by the government could be scrutinized similarly to the search conducted in *Kyllo*.

In *Kyllo*, the Supreme Court held that the government's use of thermal imaging technology, "a device not in general public use," to see through the walls of defendant's house, constituted a search.[213] Applying the reasoning of *Kyllo* to the encryption hypothetical, the government would need to obtain a probable cause warrant before breaking the device's encryption absent a specified exception.

C. *Areas for Future Investigation and Other Considerations*

Detractors of this framework might suggest that it presents too many practical impediments for law enforcement to conduct their work effectively. While this is an important consideration, "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[214] Further, the Supreme Court's job is not to aid law enforcement but, rather, be the "guardian and interpreter of the Constitution."[215] Even still, imposing a probable

[210] Jones, 565 U.S. at 409.

[211] Kyllo*,* 533 U.S. at 32–33 (citing Katz v. United States, 389 U.S. 347, 353 (1967)).

[212] *See generally* Panzarino, *supra* note 2; TECHNICAL SUMMARY, *supra* note 22; EXPANDED PROTECTIONS TECHNOLOGY, *supra* note 22.

[213] Kyllo*,* 533 U.S. at 34.

[214] Carpenter v. United States, 138 S. Ct. 2206, 2214 (citing United States v. Di Re, 332 U.S. 581 (1948)).

[215] *About the Court*, SUP. CT. U.S., https://www.supremecourt.gov/about/about.aspx [https://perma.cc/7D88-KBAQ].

cause warrant standard for encrypted data does not make combating crime impossible. As the Court explained in *Riley*:

> [w]e cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones . . . can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost. Our holding, of course is not that the information on a cell phones immune from search; it is that a warrant is generally required . . .[216]

A second critique of this framework is that it does not necessarily solve the privacy problems posed in Apple's new updates. Specifically, one could highlight that the SCA exempts ECPs disclosure to NCMEC and requires ECPs to cooperate with law enforcement generally.[217] To reiterate, the intention of this framework is *not* to discourage CSAM combating by private parties or any other lawful assistance to law enforcement. Rather, it seeks to restore the Fourth Amendment's original promise to the digital age in the absence of legislative efforts. Here, only encrypted files would receive additional protections under this framework, courts retain their ability to issue as many probable-cause warrants as they see fit, and exceptions to the law enforcement's warrant requirement still exist.

One potential area for future investigation is addressing and expounding upon where and when individuals have a REP in their encrypted smartphone data. At present, this framework only attempts to reconcile the paradigmatic incongruities between the ECPA and the Fourth Amendment; and it presents one possible path forward. Room for exploration does not offset the merits of this exploratory thought experiment.

CONCLUSION

The drama behind Apple's NeuralHash controversy brings the balance between privacy and security to the forefront of society's debate about the role of private companies in combatting social ills. The novel nature of Apple's client-side scanning in NeuralHash, as well as its on-device machine learning in the Messages app, hold significant implications for individuals' REP in the contents of their electronic files and communications from their smartphones. These privacy concerns implicate both the Fourth Amendment and the

[216] Riley v. California, 573 U.S. 373, 401 (2014).

[217] 18 U.S.C. §§ 2702(b)(6)–(8); 18 U.S.C. §§ 2702(c)(4).

ECPA, two important bodies of law that impose inconsistent requirements and provide conflicting messages to the judiciary. In keeping with the Supreme Court's Fourth Amendment jurisprudence, this paper proposes that the Supreme Court treat encryption of electronic communications and files from smartphones as akin to the physical walls of one's home in a search context. This framework represents an amalgamation of disparate Fourth Amendment doctrine to assert one's privacy interests in the contents of their electronic files and communications from personal smartphones where the *Katz* test alone may fall short.