Solitude Lost? Preserving the Fourth Amendment in the Age of the Metaverse

ABSTRACT

The Metaverse—a virtual reality platform developed by social media giant Meta Platforms, Inc. (formerly Facebook, Inc.)—promises to fundamentally alter the age-old structure of global society. Specifically, the Metaverse seeks to blend physical, virtual, and augmented realities together through a complex web of digital spaces, wearable technology, and technological synergy. Through its dual goals of "connecting people" and fostering a "feeling of presence" for Metaverse users, Meta may ultimately make virtual reality participation an unavoidable aspect of daily life. Yet despite the Metaverse's broad implications for user privacy, the current protections afforded to consumers are wholly insufficient. The Fourth Amendment, a historic symbol of the United States' commitment to individual privacy, is improperly equipped to restrain the probing reach of virtual reality. Moreover, current statutory safeguards, such as those provided in the Stored Communications Act (SCA), grant weak protections that are easily subverted. As a result, users operating in the Metaverse space—which could soon become an extension of the physical world—may be forced to relinquish their individual privacy.

This Note argues that such a future is both inconsistent with historic US values and patently unacceptable. To maintain the longstanding privacy protections that undergird the Fourth Amendment, this Note contemplates two distinct solutions with both judicial and legislative perspectives in mind: (1) that the Supreme Court extend its 2018 decision in Carpenter v. United States *to provide Fourth Amendment protections to data collected through Metaverse interactions, or (2) that the US Congress amend the SCA to constrain warrantless access to Metaverse data.*

TABLE OF CONTENTS

As modern technology continues to erode traditional social frameworks,[1] the United States draws nearer to a momentous inflection point. Rapid technological developments, coupled with the proliferation of "Big Data,"[2] have cast significant doubt upon the resilience of

1. *See generally* Shira Ovide, *Tech Won. Now What?*, N.Y. TIMES (Dec. 28, 2021), https://www.nytimes.com/2021/12/23/technology/tech-won-now-what.html [https://perma.cc/K36Y-SXJC] (explaining that "we live through tech" as technology becomes increasingly intertwined with day-to-day life); Matthew Kitchen, *20 Ways 2020 Changed How We Use Technology Forever*, WALL ST. J. (Oct. 23, 2020, 3:06 PM), https://www.wsj.com/articles/20-ways-2020-changed-how-we-use-technology-forever-11603479962 [https://perma.cc/XQ8E-QKH8] (arguing that the use of technology will be forever altered by the COVID-19 pandemic).

2. Kenneth Cukier & Victor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World*, 92 FOREIGN AFFS. 28, 28 (2013).

longstanding constitutional values.[3] For example, the introduction of tech-based policing has placed the Fourth Amendment's protection against "unreasonable searches and seizures"[4] under near-constant strain.[5] Certain tools, like geofencing and automatic license plate readers (ALPRs), have given law enforcement agencies easy access to citizens' personal information—data that can later be utilized to track down witnesses and potential criminal suspects.[6] Other, more innocuous technologies are similarly exploited for policing purposes, such as data generated from cellphone location information.[7] As a result, legal scholars have expressed concern over the Fourth Amendment's ability to protect citizens from government-sanctioned intrusions that utilize new and burgeoning technologies.[8]

Working within the limitations of its authority to interpret existing law, the judicial system tends to be "poorly suited to generate effective rules regulating criminal investigations involving new technologies."[9] Despite the unavoidable need to address the constitutional implications of modern technologies, judges are often unable to fully appreciate the technological intricacies and repercussions of their decisions.[10] This technological unfamiliarity often results in the imposition of overly formalist doctrines that can persist for decades before correction.[11] Thus, legislatures are better equipped to resolve technological concerns for three reasons: (1) "legislatures typically create generally applicable rules ex ante, while courts tend to create rules ex post"; (2) legislatures are not bound by stare decisis, and are therefore more flexible; and (3) "legislative rules tend to be the product of a wide range of inputs."[12]

---

3. *See* LAURA HECHT-FELELLA, THE FOURTH AMENDMENT IN THE DIGITAL AGE, BRENNAN CTR. FOR JUST. 1, 3 (2021).

4. U.S. CONST. amend. IV; *see* HECHT-FELELLA, *supra* note 3.

5. *See* HECHT-FELELLA, *supra* note 3, at 3.

6. *See* Reed Sawyers, *For Geofences: An Originalist Approach to the Fourth Amendment*, 29 GEO. MASON L. REV. 787, 792–93 (2022); Michael E. Fisher, *Ohio is Jonesing for Automatic License Plate Readers: Why This May Violate Your Fourth Amendment Rights and What the Ohio Legislature Should Do About It*, CLEV. ST. L. REV. 329, 330–31 (2016).

7. *See*, *e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

8. *See*, *e.g.*, HECHT-FELELLA, *supra* note 3.

9. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858 (2004) [hereinafter Kerr, *The Fourth Amendment*].

10. *Id.* at 858–59.

11. Ric Simmons, *The New Reality of Search Analysis: Four Trends Created by New Surveillance Technologies*, 81 MISS. L.J. 991, 994 (2012).

12. Kerr, *The Fourth Amendment*, *supra* note 9, at 868, 871, 875.

Yet despite the apparent benefits of legislative authority, some academics have pressed for judicial oversight in lieu of legislative involvement.[13] Specifically, in the context of digital searches, scholars argue that "courts . . . may hold the comparative institutional advantage," as Fourth Amendment concerns are often not immediately apparent, making "an interstitial judicial decision-making approach . . . preferable."[14] Moreover, digital searches are burdened by the lack of an "easy solution," making the court's ex post analysis preferable to the legislature's ex ante approach.[15] These opposing views—legislative supremacy and judicial involvement—form the necessary backdrop for analyzing the privacy issues presented by the advent of the Metaverse.[16]

It is important to note that the rise of the Metaverse implicates two distinct issues with respect to the right to privacy: (1) infringement upon traditionally private spaces, and (2) development of newfound privacy expectations. The Metaverse, like geofencing and ALPRs, can generate data via user interactions that may encroach upon consumers' constitutional rights.[17] For example, as users navigate the Metaverse, the platform's underlying infrastructure gathers "reams of data" revealing how users behave, who they talk to, and with whom they transact.[18] While this mechanism may perturb some consumers on its own, the real constitutional dilemma arises from the potential for police access of private user data—a practice which, given the proposed size and scope of the Metaverse, resembles the collection and examination of cellphone location information.[19] This data can reveal information about users' homes and other traditionally private spaces, thereby providing law enforcement with a view into users' private lives.[20] Additionally, the Metaverse may create newfound expectations of

13. *See*, *e.g.*, Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, YALE J.L. & TECH. 120, 120 (2007).

14. *Id.*

15. *Id.*

16. *Id.*; Kerr, *The Fourth Amendment*, *supra* note 9, at 868, 871, 875; David Uberti, *Come the Metaverse, Can Privacy Exist?*, WALL ST. J. (Jan. 4, 2022, 5:30 AM), https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206 [https://perma.cc/7YZJ-64C2].

17. *See* Jon M. Garon, *Legal Implications of a Ubiquitous Metaverse and a Web3 Future*, 106 MARQ. L. REV. 163, 241–42 (2022); *see also* Sawyers, *supra* note 6; Fisher, *supra* note 6.

18. *See* Uberti, *supra* note 16.

19. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

20. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, YOUTUBE (Oct. 28, 2021), https://www.youtube.com/watch?v=Uvufun6xer8&t=339s [https://perma.cc/A96G-4L5V] (describing how the Metaverse could record the physical interior of someone's home).

privacy within its digital spaces, particularly as users begin to rely upon the platform more extensively.[21]

Though similar virtual reality platforms predate the Metaverse, the sheer scope of the Metaverse and its data collection practices dwarfs that of its predecessors.[22] Thus, in approaching the privacy issues that this new technology will create, it is imperative to weigh the potential costs and benefits of legislative versus judicial involvement.[23] While it is nearly impossible to predict what technologies lie beyond the Metaverse, the possibility for further development undoubtedly exists.[24] It is essential to remain cognizant of the imminent arrival of even more intrusive technological platforms and, consequently, how lawmakers, citizens, and courts can anticipate and address them.

This Note explores the history of the right to privacy and its relationship to the Metaverse, a digital world designed by Meta Platforms, Inc. (formerly Facebook, Inc.).[25] Specifically, this Note addresses the ability of law enforcement agencies to access private data that the Metaverse collects from its consumers. Section II outlines the features of the proposed Metaverse, its potential impact on the US socioeconomic landscape, and a history of the Fourth Amendment. Section III addresses the shortcomings of both modern Fourth Amendment jurisprudence and the SCA in preserving the right to privacy. Section IV outlines two contemplated solutions—one legislative and one judicial.

---

21. *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619–21 (2011) (discussing the impact of the Internet's emergence as a "seamless part of the real world") ("[A] future is nearly upon us that will make it impossible to preserve the privacy even of traditional Fourth Amendment bastions, such as the home, without considering the intertwined effects of technological and social change.").

22. Uberti, *supra* note 16.

23. *See* Trepel, *supra* note 13; Kerr, *The Fourth Amendment*, *supra* note 9, at 868, 871, 875.

24. Saeed Elnaj, *The Realities and Future of the Metaverse*, FORBES (Sept. 30, 2022, 9:00 AM), https://www.forbes.com/sites/forbestechcouncil/2022/09/30/the-realities-and-future-of-the-metaverse/?sh=454251e438db [https://perma.cc/XBT8-CYEW]; *see* José Vida Fernández, *Introduction: The Risk of Digitalization: Transforming Government into a Digital Leviathan*, 30 IND. J. GLOB. LEGAL STUD. 3, 3–4, 13 (2023).

25. Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Nov. 10, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html [https://perma.cc/VG4Z-DNFJ].

I. BACKGROUND

A. The Creation of Virtual Worlds and the Potential for a Singular Reality

While the Metaverse is potentially the broadest application of digital reality to date,[26] "virtual worlds" have existed for decades.[27] At their core, virtual worlds are "fictitious environment[s] created by computer software [that enable] users to interact with other users and with the software itself using two- or three-dimensional figures called Avatars."[28] Beginning in the late 1980s with the creation of Multi-User Dungeons (MUDs), early virtual worlds functioned as simple text-based video games that resembled little more than crude chatrooms.[29] While these worlds began as small-scale digital platforms wherein "a plurality of [people could] interact with the world and each other," they have since evolved "to become major hubs of entertainment, education, and community."[30]

The technological infrastructure that MUDs introduced ultimately paved the way for the creation of Massively Multiplayer Online games (MMOs) like *World of Warcraft* and *The Elder Scrolls Online*.[31] Yet unlike MUDs, MMOs involve advanced interactions between millions of users within the digital domain.[32] Within these densely populated spaces, users can exchange virtual goods with one another.[33] As a result, many contemporary MMOs contain robust digital marketplaces in which participating consumers may purchase "items, land, and even characters from one another using virtual currency."[34]

---

26. *See*, *e.g.*, Zoe Weinberg, *The Metaverse Is Coming, and the World Is Not Ready for It*, N.Y. TIMES (Dec. 2, 2021), https://www.nytimes.com/2021/12/02/opinion/metaverse-politics-disinformation-society.html [https://perma.cc/7TFX-JC6B].

27. *See* Richard A. Bartle, *Virtual Worldliness: What the Imaginary Asks of the Real*, 49 N.Y.L. SCH. L. REV. 19, 20–22 (2004–05).

28. Nachshon Goltz, *"ESRB Warning: Use of Virtual Worlds by Children May Result in Addiction and Blurring of Borders" – The Advisable Regulations in Light of Foreseeable Damages*, 11 U. PITT. J. TECH. L. & POL'Y 2, 4 (2010).

29. Fred Williamson, *Multi-User Dungeons (MUDs): What are They? And How to Play*, MEDIUM (Jul. 4, 2020), https://medium.com/@williamson.f93/multi-user-dungeons-muds-what-are-they-and-how-to-play-af3ec0f29f4a [https://perma.cc/5U4X-F7Y5]; *see* Bartle, *supra* note 27, at 20.

30. Bartle, *supra* note 27, at 19.

31. Williamson, *supra* note 29.

32. Sharon K. Lowry, *Property Rights in Virtual Reality: All's Fair in Life and Warcraft?*, 15 TEX. WESLEYAN L. REV. 109, 111 (2008).

33. *See* James Bonar-Bridges, *Regulating Virtual Property with EULAs*, 2016 WIS. L. REV. FORWARD 79, 80–81 (2016).

34. *See id.* at 80.

The injection of market forces into virtual reality has thus served to further complicate the notion of digital space.[35] Now, these worlds serve not only as a method of communication but also as a platform for transacting with other users.[36]

These new, immersive phenomena are bolstered by the fact that digital reality can "spill over" into real life as the borders between the two erode—creating a single, blended existence.[37] Virtual world users routinely "think of situations from the game while not online," with many experiencing dreams tied to the digital reality.[38] With this prolonged exposure to virtual worlds, users place themselves in danger of developing addictive tendencies that may lead to excessive consumption and, ultimately, symptoms of withdrawal.[39] In fact, a comprehensive study of the once-popular MMO *Second Life* revealed that "the longer the [human user] used the virtual world, the more they reported that *Second Life* offers them a better life experience than their real life."[40] Thus, to some, virtual worlds are not merely supplements to "real" life, but are instead unavoidable aspects of life itself.[41] However, unlike these prior MMOs, the Metaverse reaches even further into the lives of its users by offering them places to transact, work, socialize, and learn, potentially exacerbating these addictive ties and making participation unavoidable.[42]

B. Introducing the Metaverse

The Metaverse, in many respects, appears to symbolize the next step in the evolution of the "virtual world" phenomenon. The vision for the Metaverse, as outlined by Meta Chief Executive Officer Mark Zuckerberg, is a hyper-expansive digital universe that fully integrates virtual, augmented, and physical realities.[43] At the core of Meta's efforts is the desire to "communicate . . . across different layers of reality."[44] These layers, according to Zuckerberg, are threefold: (1) the virtual

35. *See id.*; Lowry, *supra* note 32, at 115–17.

36. *See* Bonar-Bridges, *supra* note 33, at 80.

37. *See* Goltz, *supra* note 28, at 16.

38. *See id.*

39 *See id.* at 9–10.

40 *Id.* at 16–17.

41 *See*, *e.g.*, *id.*

42 *See id.*; Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

43 *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

44 *Id.*

space; (2) physical reality; and (3) a hybrid plane known as augmented reality, wherein the physical world is supplemented by virtual objects resembling holograms.[45] Thus, the erosion of the borders between "the digital" and "the real" appears poised to hasten.[46] But the scope of the proposed Metaverse has left some experts concerned as the technologies necessary to achieve this vision—namely augmented reality (AR) glasses and virtual reality (VR) domains—will require "reams of data showing how users interact with their surroundings in fictional worlds, digital workplaces, virtual doctors' appointments, and elsewhere."[47] Ultimately, what the Metaverse will come to achieve is incalculable, but its accomplishments will invariably implicate extensive intrusions into the real world.

1. Social Connectivity

Meta's leadership has indicated in the past that the ultimate goal of the company is to "connect people" with one another.[48] As Zuckerberg describes in the Metaverse announcement video,

> [Users are] going to be able to move across . . . different experiences on all kinds of different devices, sometimes using virtual reality so [they] are fully immersed, sometimes using augmented reality glass so [they] can be present in the physical world as well, and sometimes on a computer or a phone so [they] can quickly jump into the Metaverse from existing platforms.[49]

Through this network of enmeshed realities, Meta hopes to foster a "feeling of presence" throughout the Metaverse that will allow users to feel connected to the digital space.[50] Integral to the success of this plan is Horizon, the core social platform that allows people to create and interact in the Metaverse.[51] Within Horizon, several smaller platforms exist that allow for greater specialization: Horizon Home is a tool focused exclusively on developing the user's digital home space; Horizon Worlds allows users to build and access virtual "worlds," as well as engage with other users; and Horizon Workrooms serves as the

---

45 *Id.*

46 *See* Goltz, *supra* note 28, at 14–17.

47. Uberti, *supra* note 16.

48. *See*, *e.g.*, Kurt Wagner, *Facebook is Defending Itself Again After an Internal Memo Suggested Growth was More Important than User Safety*, VOX (Mar. 29, 2018, 7:21 PM), https://www.vox.com/2018/3/29/17178092/facebook-boz-memo-growth-safety [https://perma.cc/PF7S-WRMP]; *About Meta*, META, https://about.meta.com/ [https://perma.cc/R65Q-4YJQ] ("Meta builds technologies that help people connect, find communities and grow businesses.").

49. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

50. *Id.*

51. *See id.*

primary mechanism for creating digital offices and other working spaces.[52] Broadly, Horizon is "Meta's universe in the [M]etaverse."[53]

Even while users are operating in the Metaverse's virtual spaces, they can connect with friends, family, coworkers, and others who occupy other planes of reality.[54] As displayed in the Metaverse announcement video, it is possible for users within the VR space to contact users in the physical reality.[55] Using Meta's Messenger application, Metaverse consumers can use their digital avatars to call or video chat with individuals in the "outside world."[56] Meta's efforts deliberately blur the boundaries between physical and virtual realities to facilitate communications between its users.[57] As a result, the Metaverse may soon become fully integrated within the lives of its users; as consumers can hop in or out of the Metaverse at their leisure to communicate with their friends, participation becomes increasingly unavoidable for the general public.[58]

2. Commerce, Entertainment, and Work

Much like the virtual worlds that preceded it, the Metaverse also aims to foster a robust digital marketplace wherein creators can sell digital objects, services, and experiences.[59] The capacity for economic growth within the Metaverse is massive, with Citi estimating that the market's value could reach between eight and thirteen trillion dollars by 2030.[60]

---

52. *See Meta Horizon Home*, META, https://www.meta.com/help/quest/articles/in-vr-experiences/social-features-and-sharing/meta-horizon-home/ [https://perma.cc/S72Q-8T3W] (last visited Jan. 27, 2024); *Travel to a friend in Meta Horizon Worlds*, META, https://www.meta.com/help/quest/articles/horizon/explore-horizon-worlds/travel-to-a-friend-in-horizon/ [https://perma.cc/CCJ6-CK3H] (last visited Jan. 27, 2024); *Learn about Meta Horizon Workrooms*, META, https://www.meta.com/help/quest/articles/horizon/getting-started-in-horizon-workrooms/learn-about-workrooms/ [https://perma.cc/T9K5-GZZ2] (last visited Jan. 27, 2024).

53. Kashmir Hill, *This is Life in the Metaverse*, N.Y. TIMES (Oct. 7, 2022), https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html [https://perma.cc/CY76-GLD7].

54. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

55. *See id.*

56. *See id.*

57. *See id.*

58. *See id.*; Hill, *supra* note 53.

59. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

60. Will Canny, *Citi Sees Metaverse Economy as Large as $13T by 2030*, COINDESK (Apr. 1, 2022, 6:45 AM CDT), https://www.coindesk.com/business/2022/04/01/citi-sees-metaverse-economy-as-large-as-13t-by-2030/ [https://perma.cc/RU6Y-U9XS].

In addition to a dynamic system of digital commerce, the Metaverse is also designed to provide spaces for entertainment opportunities and work obligations.[61] For example, in the Metaverse announcement video, a young woman decides to attend a concert with her friend.[62] She suddenly appears beside her friend, who is attending the concert physically, as a hologram.[63] Using AR glasses, the two companions can see, communicate, and interact with one another.[64] From there, they can engage with the augmented reality projected around them, or enter into a VR room to attend an after-party.[65] Thus, the possibilities for cross-platform engagement appear endless.[66]

Similarly, the Metaverse is expanding the possibility for remote work for employees across the world.[67] Digital avatars will be able to attend work meetings in dedicated VR spaces,[68] and virtual home offices will be equipped with central workstations akin to physical computers.[69] Through these tools, Metaverse users will be able to develop and maintain documents, attend work meetings, and communicate directly with their work colleagues.[70]

3. Privacy and Security

In his Metaverse announcement video, despite detailing the extensive user opportunities, Zuckerberg hardly discussed specific protections for those users' privacy and safety.[71] Rather, Zuckerberg merely made vague mention of the notion that "privacy and safety need to be built into the Metaverse from day one."[72] He further contended that the Metaverse will require "ecosystem building, norm-setting, and

61. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *See id.*

67. *Id.*

68. *See id.*; John Herrman & Kellen Browning, *Are We in the Metaverse Yet?*, N.Y. TIMES (Oct. 29, 2021), https://www.nytimes.com/2021/07/10/style/metaverse-virtual-worlds.html#:~:text=If%20you%20own%20a%20non,into%20the%20neighbor-hood%20of%20metaversality. [https://perma.cc/G7EH-9ECG].

69. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

70. *See id.*

71. *See id.*

72. *Id.*

new forms of governance" to ensure that the privacy of its users remains secure, but failed to elaborate on what these goals mean.[73]

The Metaverse's lack of specified privacy assurances has not prevented the company from targeting the most personal aspects of users' lives.[74] First, through its augmented reality program—which relies chiefly on physical AR glasses containing highly complex sensors—the Metaverse may map and monitor aspects of users' physical living quarters.[75] By tracking both surrounding objects and the user's eye movements, these AR glasses will have the ability to perform what Meta calls "information indexing."[76] While Meta claims the requisite technology is currently out of reach, the company emphasized that this process will ultimately allow the glasses to access data from three-dimensional scans to better understand the location, texture, geometry, and function of different physical objects.[77] In sum, Meta's AR glasses have the capacity to create digital maps of users' homes by cultivating data regarding what objects the user owns and where they are located in the home.[78]

Second, in the VR space, "Meta . . . asks Horizon users to consent to having their audio recorded."[79] If users refuse consent, they are prohibited from talking in Horizon, a consequence that will carry significant weight as the Metaverse's VR component becomes increasingly integrated into daily life.[80] While the company claims that the audio data are stored locally in each user's headset, Meta can access the information at a moment's notice.[81]

Finally, by tracking its users' precise eye movements, Meta's gathered information can provide insight into users' thoughts, feelings,

---

73. *Id.*

74 *See generally* Jenna Furman, *I Know What You're Thinking: Brain Imaging and Mental Privacy*, 30 SYRACUSE J. SCI. & TECH. L. 160, 170–71 (2014) (highlighting the "ethical concerns regarding the use of brain imaging and its implications on the person's right to privacy"); Thiago M. Coelho & Carol M. Bast, *Citizens Policing the Police: An Evaluation of Citizens Recording Police Officers and Eavesdropping Laws*, 51 CRIM. L. BULL. (2015) (explaining that the right to privacy in conversation exists when a reasonable expectation of privacy exists); Thomas P. Crocker, *The Fourth Amendment at Home*, 96 IND. L.J. 167, 168 (2020) (contending that the home is "a refuge, a domain of personal privacy").

75. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

76. *See id.*

77. *Id.*

78. *See id.*

79. Hill, *supra* note 53.

80. *See id.*

81. *Id.*

and emotions.[82] Because "users may look differently at other players in a game . . . than they would at the avatar of a boss they don't like," specific photos or videos may trigger an emotional response from the user.[83] Certain indicators—such as a user's gaze or pupil dilation—may inadvertently reveal emotional information to Meta staff.[84] Therefore, at any given moment, Metaverse users may be subject to a discreet system of emotional tracking, which can give Meta, and any other company involved, a "unique window into users' psyches."[85] As a result, not even one's own thoughts or feelings are safe from the intrusive practices that Meta could ultimately employ.[86]

Ultimately, given the sheer scope of the Metaverse, the privacy of millions of potential users may be in jeopardy.[87] As users are pushed to participate in this ever-expanding digital world, they will, in turn, forfeit "reams of data" to the company that may be accessed and abused by federal, state, and local actors.[88] Areas that have traditionally been viewed as sacred spaces—homes, private conversations, and even one's own thoughts, feelings, and emotions—are now goldmines for data collection.[89]

C. The Fourth Amendment Framework

1. Overview and a History

The Fourth Amendment to the Constitution of the United States guarantees "[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."[90] In a broad sense, the promise contained within the text of the Fourth Amendment reflects the Framers' steadfast commitment to the maxim that "government intrusion must be

82. Uberti, *supra* note 16; David Z. Morris, *Meta Leans In to Tracking Your Emotions in the Metaverse*, COINDESK (Jan. 19, 2022, 1:14 PM CDT), https://www.coindesk.com/layer2/2022/01/19/meta-leans-in-to-tracking-your-emotions-in-the-metaverse/ [https://perma.cc/3BBL-TDBD].

83. *See* Uberti, *supra* note 16.

84. *See id.*

85. *Id.*

86. *See id.*

87. *See*, *e.g.*, *id.*; Herrman & Browning, *supra* note 68.

88. *See* Uberti, *supra* note 16.

89. *See*, *e.g.*, Crocker, *supra* note 74; Coelho & Bast, *supra* note 74; Furman, *supra* note 74; Uberti, *supra* note 16.

90. U.S. CONST. amend. IV.

carefully limited and regulated."[91] In the pre-Revolutionary United States, Crown officials conducted intrusive searches predicated upon a type of general warrant,[92] which permitted government actors to "search anywhere they pleased for any reason—or for no reason."[93] The colonists, unsurprisingly, deemed these warrants particularly offensive, prompting one activist to claim that they "made a citizen 'the servant of servants' in his own home."[94]

Beyond mere words, the permissive provisions of general warrants, along with the intrusive searches that accompanied them, ultimately inspired counteractions.[95] In a direct response to governmental overreaches, John Adams penned article XIV of the Massachusetts Constitution of 1780, which stated, in pertinent part, that:

> Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order . . . be not accompanied with a special designation of the persons or objects of search, arrest, or seizure.[96]

The language from this provision, drafted by one of the nation's most well-known Founding Fathers, bears a striking resemblance to the Fourth Amendment.[97]

Eventually, the Framers of the US Constitution enacted the Fourth Amendment to enshrine the nation's collective interest in securing privacy against arbitrary intrusion, a doctrine that the Court later incorporated against state officials in *Wolf v. Colorado* in 1949.[98] In its decision, the Court was careful to note that it deemed this right to privacy as "basic to a free society," and therefore "implicit in the concept of ordered liberty."[99] Moreover, the Court explained that searches of the home unsupported by authority of law run counter to the very notion of human rights.[100] Consequently, the retention of

---

91. Brandon R. Teachout, *On Originalism's Originality: The Supreme Court's Historical Analysis of the Fourth Amendment from Boyd to Carpenter*, 55 TULSA L. REV. 63, 70–71 (2019).

92. *See id.*

93. Thomas K. Clancy, *Annual Lecture on Search and Seizure Principles*, 76 MISS. L.J. 581, 581–82 (2006).

94. Teachout, *supra* note 91, at 71. *See also* Clancy, *supra* note 93, at 582.

95. *See* Teachout, *supra* note 91, at 71.

96. MASS. CONST. art. XIV; *see* Teachout, *supra* note 91.

97. *See* Clancy, *supra* note 93 (asserting that the Fourth Amendment was inspired by Article Fourteen of the Massachusetts Constitution).

98. Wolf v. Colorado, 338 U.S. 25, 27–28 (1949).

99. *Id.*

100. *Id.* at 28.

privacy in areas traditionally deemed personal—like the home—was of paramount importance.[101]

Ultimately, the notion of an individual's right to privacy, particularly in areas that have traditionally been considered personal, has deep historical roots in the United States.[102] From colonial tirades against general warrants, through Article Fourteen of Massachusetts' Declaration of Rights, to the Fourth Amendment, there is an unmistakable chain of concern for individual privacy.[103] This notion of privacy, which the Framers so fervently treasured, was designed to protect areas of great confidentiality—including the home.[104]

2. Modern Fourth Amendment Jurisprudence

It is important to note that the Fourth Amendment prohibits only unreasonable searches and seizures.[105] In light of this qualification, and given the United States' strong historic commitment to privacy in one's home and similar settings,[106] the question remains: how far does the right to privacy extend today? To answer that question, one must turn to the seminal case of *Katz v. United States*.[107]

The defendant in *Katz* had been charged with and convicted of the transmission of gambling information via telephone, an act prohibited by federal statute.[108] To catch Katz, the Federal Bureau of Investigation installed electronic listening and recording devices to the exterior of the public telephone booth that Katz utilized.[109] The Court was quick to note that, despite the public location of the telephone booth and the lack of *physical* intrusion by the government, Katz's conduct was safeguarded by the Fourth Amendment.[110]

The Court deliberately noted that the Fourth Amendment "protects people, not places."[111] With this statement, the Court made clear that the Fourth Amendment is, above all else, designed to protect

---

101 *See id.* at 27–28.

102. *See*, *e.g.*, MASS. CONST. art. XIV; Teachout, *supra* note 91, at 70.

103 *See* Teachout, *supra* note 91, at 70–71; MASS. CONST. art. XIV; U.S. CONST. amend. IV; Clancy, *supra* note 93.

104 *See* Teachout, *supra* note 91, at 71; *Wolf*, 338 U.S. at 27–28.

105. Grady v. North Carolina, 575 U.S. 306, 310 (2015).

106. *See* Clancy, *supra* note 93.

107. 389 U.S. 347 (1967).

108. *Id.* at 348.

109. *Id.*

110. *Id.* at 351–52, 359.

111. *Id.* at 351.

an individual's expectation of privacy.[112] In turn, the Court departed from a Fourth Amendment jurisprudence steeped in property rights.[113] In previous decisions, the key inquiry was whether the government had made a physical intrusion into a suspect's house, person, papers, or effects.[114] For example, while government officers could tap into public telephone wires to listen to private conversations,[115] they could not attach a "spike mike" to the heating duct of a suspect's house as a means to eavesdrop.[116] While both cases involved police officers overhearing private dialogue, only the latter was found constitutionally violative due to the officers' "unauthorized physical penetration" into the suspect's home.[117]

While the right to privacy has deep roots in Fourth Amendment jurisprudence, it took a significant amount of time for the Court to fully embrace the totality of the right's coverage.[118] In a shift away from its property-based understanding of the Fourth Amendment, the Court adopted its new, privacy-focused model.[119] However, "[a]lthough the majority pronounced a departure from the origin of the Fourth Amendment, it failed to establish a clear standard that could be followed in subsequent cases" to determine when a warrant is required.[120] To fill this gap, Justice Harlan formulated the now-ubiquitous two-pronged *Katz* test: "first, that a person [has] exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[121] Today, whatever an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[122] Ultimately, if a suspect's reasonable expectation of

112. *See id.*; Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 5 (2012).

113. *See* Sean M. Kilbane, *Drones and Jones: Rethinking Curtilage Flyover in Light of the Revived Fourth Amendment Trespass Doctrine*, 42 CAP. U. L. REV. 249, 259 (2014).

114. *See id.*

115. *See* Olmstead v. United States, 277 U.S. 438, 463–64 (1928).

116. *See* Silverman v. United States, 365 U.S. 505, 509 (1961).

117. *See id.* at 509–10; *Olmstead*, 277 U.S. at 456, 466.

118. *See* Katz v. United States, 389 U.S. 347, 352–53 (1967); Randal Rust, *Writs of Assistance*, AM. HIST. CENT. (Oct. 27, 2023), https://www.americanhistorycentral.com/entries/writs-of-assistance/ [https://perma.cc/AVB4-NN36] (recognizing that the individual right to privacy existed independent of personal property over 200 years after James Otis' tirade).

119. *See* Arcila, *supra* note 112.

120. Kilbane, *supra* note 113, at 261.

121. *Katz*, 389 U.S. at 361 (Harlan, J., concurring); HECHT-FELELLA, *supra* note 3, at 4.

122. *See Katz*, 389 U.S. at 351.

privacy is infringed upon, the subsequent search or seizure is unreasonable, and therefore unconstitutional, without a warrant.[123]

3. Knowing Exposure Doctrine

Despite *Katz*'s careful description of one's reasonable expectation of privacy, the Court also noted that the Fourth Amendment does not protect what a person knowingly exposes to the public.[124] If a suspect has "knowingly exposed" certain information to the public at large, they no longer have a reasonable expectation of privacy with respect to that information.[125] For example, in *United States v. Knotts*, the Court recognized that individuals enjoy a "diminished expectation of privacy" in vehicles due to the public nature of roads.[126] The Court reasoned that when an individual has travelled along a roadway, he or she has "voluntarily conveyed to anyone who wanted to look the fact that [he or she] was travelling over particular roads in a particular direction."[127] Thus, the concept of "knowing exposure" serves as a limiting principle on the protections provided by the Fourth Amendment.[128]

4. The Third-Party Doctrine

Much like the theory of "knowing exposure," the third-party doctrine dictates that "individuals have no legitimate expectation of privacy in information that they voluntarily share with third parties."[129] Further, the third-party doctrine applies "regardless of whether [the suspect] intended for the government to have access to the [information]."[130] As a result, government officials may conduct a warrantless search and seizure of information from a third-party source, even if they would require a warrant to search the suspect directly.[131]

---

123. *See id.* at 362–63 (White, J., concurring). While certain exceptions exist to this general requirement—like, for example, the constitutional validity of warrantless searches during exigent circumstances—these exceptions are not relevant for the purposes of this Note. *See*, *e.g.*, Kentucky v. King, 563 U.S. 452, 460 (2011).

124. *Katz*, 389 U.S. at 351.

125. *See* Beth Shane, *After "Knowing Exposure": First and Fourth Amendment Dimensions of Drone Regulation*, 73 N.Y.U. ANN. SURV. AM. L. 323, 325 (2018).

126. 460 U.S. 276, 281 (1983).

127. *Id.* at 281–82.

128. *See* Shane, *supra* note 125, at 325–26.

129. *See* HECHT-FELELLA, *supra* note 3, at 4.

130. *Id.* at 4–5.

131. *See id.* at 5.

The third-party doctrine is best articulated in two cases: *United States v. Miller* and *Smith v. Maryland*.[132] In *Miller*, the defendant had copies of checks and other bank records seized by government officials investigating his involvement in a tax fraud scandal.[133] The Court held that because the defendant had forfeited these files to a third party, he no longer retained a reasonable expectation of privacy over the files.[134] Moreover, the Court noted that it did not matter that the defendant made the records available to the banks for a limited purpose and therefore did not intend for the government to access them.[135] Rather, the Court noted the documents contained "only information voluntarily conveyed to the banks and exposed to their employees" and therefore rejected the defendant's Fourth Amendment claim.[136]

Similarly, in *Smith*, the Court found that the defendant lacked a reasonable expectation of privacy over telephone numbers he had dialed.[137] The officers in *Smith* installed a pen register[138] device at the telephone company's headquarters to maintain a record of the calls the defendant had logged.[139] In arriving at its conclusion, the Court reasoned that "[a]ll subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial."[140] Ultimately, the use of a more technologically driven form of surveillance did not give the Court pause, as it adhered to *Miller*'s line of reasoning that "a person has no legitimate expectation of privacy in information [he or she] voluntarily turns over to third parties."[141]

As tech companies continue to promote digital instruments as supplements to daily life, individual consumers have begun to expose "nearly all aspects of their lives to their cell phone and internet service providers."[142] The Court has acknowledged this and has exhibited a shift in its Fourth Amendment jurisprudence to account for these

132. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

133. *See Miller*, 425 U.S. at 436.

134. *See id.* at 440, 442.

135. *See id.* at 442.

136. *See id.*

137. *See Smith*, 442 U.S. at 742.

138. A pen register is a "device . . . that traces outgoing signals from a specific phone" in order to produce a list of contacted phone numbers. *Pen Register*, CORNELL L. SCH., https://www.law.cornell.edu/wex/pen_register [https://perma.cc/TU3M-LXXW] (last visited Jan. 27, 2024).

139. *See Smith*, 442 U.S. at 741.

140. *Id.* at 742.

141. *Id.* at 743–44.

142. *See* Shane, *supra* note 125, at 326.

developments—indicating that the third-party doctrine is not plenary in nature.[143]

In *Carpenter v. United States*, decided in 2018, the US Supreme Court grappled with the admissibility of cell-site location information (CSLI) data that had been acquired by federal law enforcement officers without a warrant supported by probable cause.[144] An investigation into a string of robberies prompted the officers to secure the call records of one of the identified suspects.[145] Using this information, the officers determined that the suspect had previously contacted the defendant.[146] Pursuant to the SCA, the prosecutors then applied for court orders to obtain the defendant's phone records.[147] The prosecutors secured two orders from federal magistrate judges that required the defendant's wireless carriers to divulge over 150 days' worth of CSLI data from Carpenter's carriers.[148]

The CSLI data had originally been collected and stored by the defendant's wireless carriers for "their own business purposes."[149] As the Court correctly noted, modern CSLI practices generate "vast amounts" of precise data through near-constant scans of the surrounding environment.[150] Yet, even though the defendant had technically surrendered this data to his third-party service provider, the Court declined to extend the precedents of *Miller* and *Smith*, as it distinguished between prior technologies and modern CSLI data.[151] Thus, the Court concluded that government officials "must generally obtain a warrant supported by probable cause before acquiring such records."[152] Given *Carpenter*'s narrow holding, however, questions remain as to its applicability to other modern technologies.[153]

Carpenter's transformative outcome has led to a variety of interpretations regarding the scope of its applicability.[154] In his *Carpenter* dissent, Justice Kennedy characterized the five key factors to the majority's decision as: (1) comprehensiveness; (2) intimacy; (3)

143. *See* HECHT-FELELLA, *supra* note 3, at 8; Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

144. *See Carpenter*, 138 S. Ct. at 2212, 2221 (2018).

145. *See id.* at 2212.

146. *See id.*

147. *Id.*

148. *Id.*

149. *Id.*

150. *See id.* at 2211, 2212.

151. *See id.* at 2217.

152. *Id.* at 2221.

153. HECHT-FELELLA, *supra* note 3, at 10.

154. *See id.* at 9–12.

expense; (4) retrospectivity; and (5) voluntariness.[155] A contrasting viewpoint isolates just three factors from *Carpenter*: "(1) 'the deeply revealing nature' of the information; (2) 'its depth, breadth, and comprehensive reach'; and (3) 'the inescapable and automatic nature of its collection.'"[156] As a result of this discord, coupled with the case's narrow, fact-specific holding, extending *Carpenter*'s logic remains a murky enterprise.[157] Yet several areas of overlap appear to emerge—namely, the information's comprehensive nature, its ability to reveal personal details, and the decision, or lack thereof, of the consumer to surrender the information.[158]

Therefore, while the *Katz* doctrine forms the basis for modern Fourth Amendment jurisprudence, its "reasonable expectation of privacy" test operates under at least two limiting principles.[159] First, when individuals knowingly expose information to the public, they do not enjoy *Katz*'s protection from state-sanctioned interference.[160] And second, traditionally, when individuals volunteer information to third parties, then they, too, may be unprotected.[161] In light of *Carpenter*, the durability of the third-party doctrine is unclear; while users of "inescapable" technologies that collect a comprehensive swath of intimate data may still enjoy privacy protections, the path forward is murky at best.[162]

---

155. *Id.* at 9; *see also Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting).

156. *See* Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 358, 370 (2019) (quoting *Carpenter*, 138 S. Ct. at 2223).

157. *See* HECHT-FELELLA, *supra* note 3, at 8 (noting that "the Court declined to explain how its holding might be applied to data or technologies other than historical CSLI").

158. *See id.* at 9–11; *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting); Ohm, *supra* note 156.

159. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); HECHT-FELELLA, *supra* note 3, at 4; Shane, *supra* note 125; United States v. Miller, 425 U.S. 435, 443 (1976).

160. *See* Shane, *supra* note 125.

161. *See*, *e.g.*, *Miller*, 425 U.S. at 443; Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

162. *See* HECHT-FELELLA, *supra* note 3, at 10; Ohm, *supra* note 156.

II. ANALYSIS

A. Subverting Traditional and Invented Expectations of Privacy

The rise of the Metaverse implicates two distinct issues with respect to the right to privacy: (1) the infringement upon traditionally private spaces like the home; and (2) the development of newfound privacy expectations.[163] In other words, not only are "traditional Fourth Amendment bastions" impacted by the Metaverse, but the digital spaces created by the platform also establish new expectations of privacy.[164] This clarification is tremendously valuable because it accounts for the plethora of ways in which technological advancements—like the Metaverse—implicate the right to privacy, particularly as these technologies grow to encompass "the full panoply of human behavior."[165]

The data collected through Metaverse interactions—including not only information regarding a person's "movements, appearance, and surroundings," but also data generated via "games, fitness programs, [and] other digital activities"—raises a number of Fourth Amendment concerns over a user's typical expectation of privacy.[166] Traditionally, the home has been viewed as a bastion of Fourth Amendment protection;[167] privacy was required to avoid making a citizen "'the servant of servants' in his own home."[168] Yet the Metaverse creeps one step closer to the realization this specter through the use of three-dimensional location scans to generate maps of users' homes.[169] Should government officials be afforded access to this data sans warrant, the ability of citizens to "retreat into [their] own home[s]" would be

163. *See* Strandburg, *supra* note 21.

164. *See id.*

165. *See id.* at 619.

166. *See* Andrea Vittorio, *Metaverse Technology Opens Up a Wider World of Privacy Concerns*, BLOOMBERG L. (Aug. 30, 2022, 4:05 AM), https://news.bloomberglaw.com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns [https://perma.cc/A8E4-XJDV]; Oriana Alexander, Wail Jihadi & Bryan Parker, *Cybersecurity, Privacy and Constitutional Concerns: Risks to Know Before Entering the Metaverse*, LAW.COM (Mar. 29, 2022, 7:00 AM), https://www.law.com/legaltechnews/2022/03/29/cybersecurity-privacy-and-constitutional-concerns-risks-to-know-before-entering-the-metaverse/?slreturn=20230110032618 [https://perma.cc/G48C-8RTP].

167. Strandburg, *supra* note 21, at 619.

168. *See* Teachout, *supra* note 91, at 71.

169. *Compare* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20 (explaining that the Metaverse's AR glasses will constantly monitor users' homes to construct digital models), *with* Teachout, *supra* note 91, at 70–71 (discussing James Otis's reverence for the sanctity of one's own home and the privacy expectations that homes inherently possess).

rendered futile.[170] The Supreme Court has made clear that "when it comes to the Fourth Amendment, the home is first among equals."[171] Consequently, government access to digital maps of users' homes appears to run counter to both traditional and modern expectations of privacy in one's "castle."[172]

Despite its status as the superlative Fourth Amendment "bastion,"[173] it is imperative to look beyond the boundaries of the home for additional privacy expectations—particularly as the Fourth Amendment "protects people, not places."[174] Thus, looking through the lens of the individual right to privacy, the Metaverse's ability to track the emotional data of its users may prove particularly violative.[175] Applying the *Katz* test,[176] one almost certainly has a subjective expectation of privacy within his or her own mind, and it seems clear that if society is prepared to accept the reasonableness of privacy in a telephone booth, expecting privacy in one's mind is a given.[177] That the Fourth Amendment ought to preserve the right to be private in one's own thoughts is hardly a novel concept.[178] For if the Fourth Amendment truly "marks a line between the government and its citizens,"[179] then government officials should not be given unfettered and unqualified access to intimate and individualized data.[180] After all, much lesser intrusions have historically been said to "place[] the liberty of every man in the hands of every petty officer."[181]

The Metaverse's impact is not restricted to traditionally private spheres like one's home or brain.[182] Rather, as the platform continues to develop for consumers to gather, communicate, and transact, one must consider what privacy protections are afforded to the users of

170. *See* Crocker, *supra* note 74, at 177–80.

171. *See* Florida v. Jardines, 569 U.S. 1, 6 (2013).

172. *See* Crocker, *supra* note 74, at 68 (discussing both the "ancient adage that a man's house is his castle" and the special emphasis that the Fourth Amendment places on "securing protections for the home . . . against unwarranted government intrusion").

173. *See* Strandburg, *supra* note 21, at 618. *See also* Teachout, *supra* note 91, at 74.

174. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

175. *See id.* at 350 (recognizing the Fourth Amendment's protection of the individual right to privacy); Uberti, *supra* note 16; Furman, *supra* note 74.

176. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

177. *See id.* at 351–52, 359.

178. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

179. Arthur Leavens, *The Fourth Amendment and Surveillance in a Digital World*, 27 J. C.R. & ECON. DEV. 709, 734 (2015).

180. *See Olmstead*, 277 U.S. at 478 (1928) (Brandeis, J., dissenting).

181. *Id.* (internal quotations omitted).

182. *See* Strandburg, *supra* note 21, at 619.

these new digital spaces.[183] In *Kyllo v. United States*, the Court rejected the assumption that "every technological means of tracking or analyzing data . . . is constitutionally reasonable without appropriate legal justification."[184] Meaning, in other words, new technologies are not immune to the warrant requirement.[185] Thus, like in *Katz*, courts must be "sensitive to the ways in which technology frames social behavior," as it may carry new, albeit subjective, expectations of privacy.[186]

This approach is particularly instructive with respect to the Metaverse, wherein users may feel secure in their digital homes or private conversations only to have their privacy marred by a government search of their data.[187] Essentially, within the new digital spaces that the Metaverse aims to provide—like Horizon Home and Horizon Worlds—users may begin to develop expectations of privacy that may not currently enjoy legal recognition.[188] Furthermore, as users become increasingly dependent on VR technology, the creation of a singular reality might fortify users' new expectations of privacy.[189] Consequently, as the Metaverse continues to blend virtual, physical, and augmented realities,[190] it endangers the individual consumer's right to privacy by subverting traditional notions of privacy and refusing to observe newly developed privacy expectations.[191]

B. Ineffective Protections for Consumers

1. Data Use Agreements

Data use agreements have traditionally operated as the key safeguard against potential subversions of consumer privacy.[192] Generally, data use agreements restrict the collection and

183. *See id.* at 619–21.

184. *Id.* at 621–22 (citing Kyllo v. United States, 533 U.S. 27 (2001)).

185. *See* Strandburg, *supra* note 21, at 621–22.

186. *Id.* at 619–22.

187. *See id.* at 656 (asserting that social media are used for "very personal" activities, like those "involving medical problems, sexual concerns, or exploration of unpopular political perspectives"), 633 (contending that the Court must extend the Fourth Amendment's protections to impede government surveillance on social media platforms).

188. *See* Strandburg, *supra* note 21.

189. *See* Goltz, *supra* note 28, at 16.

190. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

191. *See* Strandburg, *supra* note 21, at 649.

192. *See* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. 8, 16–17 (2016).

dissemination of consumer information in private transactions.[193] These policies "typically tell [consumers] that the company will . . . make use of [consumers'] information only for certain specified purposes," and thereby preserve a significant portion of consumer privacy.[194] However, these policies are subject to two important restrictions that limit their effectiveness: (1) they are subject to change at the whims of the company;[195] and (2) they can be overridden by statute.[196] Therefore, despite their surface-level appeal, the restrictions in data use agreements are imperfect safeguards for consumer information due to their practical infirmities.[197]

2. The Fourth Amendment

Current Fourth Amendment jurisprudence does not provide a better alternative to protect consumers' right to privacy in the Metaverse.[198] First, the knowing exposure doctrine asserts that information "voluntarily conveyed" to the public does not enjoy Fourth Amendment protection from unreasonable searches.[199] In the Metaverse, then, certain interactions, like those held in public chatrooms and other common areas, would not carry a right to privacy as the individual would have forfeited that right by making the information accessible to the public.[200] Thus, certain Metaverse actions would be per se unentitled to constitutional protection.[201]

But the larger issue exists with respect to the third-party doctrine, which serves as a much stronger limit on the Fourth

193. *See id.*

194. *Id.* at 17.

195. *See*, *e.g.*, Kate O'Flaherty, *Facebook's New Privacy Policy—What You Need to Know*, FORBES (May 27, 2022, 10:14 AM), https://www.forbes.com/sites/kateoflahertyuk/2022/05/27/facebooks-new-privacy-policy-what-you-need-to-know/?sh=2230e6eaf84c [https://perma.cc/98FE-7PVV].

196. *See* Marcus Schlundt Bodien, *"This Meeting is Being Recorded": 'Zoom'-ing Away from the Third-Party Doctrine*, 14 DREXEL L. REV. 495, 521–22 (2022) (contending that the Stored Communications Act overrides Zoom's privacy policy and therefore allows the government to obtain data without obtaining a warrant).

197. *See* Schlundt Bodien, supra note 196.

198. *See generally*, Luiza M. Leão, *A Unified Theory of Knowing Exposure: Reconciling* Katz *and* Carpenter, 97 N.Y.U. L. REV. 1669, 1677–78 (2022) (discussing the "knowing exposure" exception to the Fourth Amendment right to privacy); Chelsea Ann Padgett, *Implications of the Third-Party Doctrine: The New Age of Digital Data and* Carpenter, 72 FLA. L. REV. 905, 914–917 (2020) (documenting several criticisms of the third-party doctrine and its hinderance of the Fourth Amendment's right to privacy).

199. *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983).

200. *See* Shane, *supra* note 125, at 346.

201. *See id.* at 346.

Amendment rights of Metaverse users.[202] The third-party doctrine asserts that once an individual conveys information to a third party, that individual has forfeited any reasonable expectation of privacy that they would have normally enjoyed.[203] Per *Smith* and *Miller*, Metaverse users, by participating in the Metaverse and voluntarily conveying their data, would relinquish any reasonable expectation of privacy with respect to that information.[204] By forfeiting this expectation of privacy, consumers no longer satisfy the *Katz* test, which may allow government officials to access their data sans warrant.[205] Thus, under the *Smith* and *Miller* line of cases, Metaverse users, by voluntarily conveying their data, are effectively without their Fourth Amendment right to privacy in this space.[206] As the use of the Metaverse becomes more integrated into contemporary society, the risks that the platform presents to individual privacy rights grow in expected and unexpected ways—both immensely dangerous.[207]

Yet following the significant blow to the third-party doctrine in *Carpenter v. United States*, which held that the third-party doctrine does not apply to the collection of CSLI data, it is unclear how this new doctrine would apply to the Metaverse specifically.[208] Privacy advocates are clamoring for a liberal application of *Carpenter* that would effectively terminate the third-party doctrine's applicability to cases involving digital technologies, but the *Carpenter* decision's interaction with the Metaverse is potentially a much deeper question.[209]

3. The Stored Communications Act

The SCA attempts to govern the privacy of stored internet communications.[210] The SCA was designed to fill the gap left by the Fourth Amendment's failure to safeguard most internet-based

202. *See* Padgett, *supra* note 198, at 910.

203. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976); Padgett, *supra* note 198, at 910.

204. *See Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–43.

205. *See Smith*, 442 U.S. at 741–42; *Miller*, 425 U.S. at 442–43; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

206. *See* Padgett, *supra* note 198, at 910–14.

207. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

208. *See* Padgett, *supra* note 198, at 923–32.

209. *See* Strandburg, *supra* note 21, at 634, 679.

210. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) [hereinafter Kerr, *Stored Communications Act*]; 18 U.S.C. §§ 2701–13.

activities.[211] Despite this goal, the SCA ultimately fails to adequately protect consumers, as it allows the government to compel disclosure of certain electronically stored information without a warrant.[212]

At the SCA's lowest threshold, the government need only a simple subpoena to compel basic subscriber information.[213] But the real issue lies within Section 2703(d), which allows the government to compel large swaths of data upon a showing of mere "reasonable grounds" to believe that the information sought is relevant to a criminal investigation.[214] For example, if the government satisfies the "reasonable grounds" showing, its officers can order the disclosure of all non-content records.[215] When coupled with prior notice, a government order under Section 2703(d) compels "*everything* except contents in temporary 'electronic storage' [for] 180 days or less."[216] The SCA only requires a full search warrant when the government wishes to compel the disclosure of content data that is in electronic storage for 180 days or less; all other types of data may be obtained without first obtaining a warrant—largely through Section 2703(d).[217]

The relaxed "reasonable grounds" standard mirrors that of reasonable suspicion, falling short of the probable cause showing required to obtain a traditional warrant.[218] And unfortunately, the government has taken full advantage of Section 2703(d)'s meager evidentiary threshold to gain access to substantial amounts of consumer-generated data, as was the case in *Carpenter*.[219]

Finally, the SCA permits officers to mandate information disclosures, and thereby overrides private data use agreements.[220] As a result, should private entities like Meta wish to impose stricter requirements on government access to data, their efforts would be in

211. *See* Kerr, *Stored Communications Act*, *supra* note 210, at 1209–10.

212. *See* Gabriel R. Schlabach, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 680 (2015); 18 U.S.C. § 2703(d).

213. Kerr, *Stored Communications Act*, *supra* note 210, at 1222.

214. *See id.* at 1222–23; Schlabach, *supra* note 212, at 712; 18 U.S.C. § 2703(d).

215. *See* Kerr, *Stored Communications Act*, *supra* note 210, at 1222; 18 U.S.C. § 2703(d).

216. Kerr, *Stored Communications Act*, *supra* note 210, at 1223 (emphasis added).

217. *See id.* at 1222–23; 18 U.S.C. § 2703(a), (d).

218. *See* Schlabach, *supra* note 212, at 700; Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

219. *See Carpenter*, 138 S. Ct. at 2212.

220. *See* Schlabach, *supra* note 212, at 680; Bodien, *supra* note 196, at 504; 18 U.S.C § 2703(b).

vain.[221] In light of the foregoing, the SCA flatly fails to protect user privacy.[222]

III. SOLUTION

This Note contemplates two separate solutions—one judicial and one legislative. First, the Supreme Court should extend the *Carpenter* decision to eliminate the effects of the third-party doctrine with respect to the collection of Metaverse data.[223] Alternatively, the US Congress should amend the SCA to raise the evidentiary threshold for government searches of Metaverse data.[224]

A. The Judicial Solution

1. Extending *Carpenter*'s Coverage

The crux of the *Carpenter* decision rests principally on three concerns: (1) the comprehensiveness of the government's surveillance practices, (2) the intimacy of the information revealed, and (3) the ability of individuals to avoid said surveillance.[225] Much like the CSLI data at issue in *Carpenter*, the data produced by the Metaverse satisfies the factors necessary for Fourth Amendment protection against warrantless searches.[226]

First, the scope of Metaverse-created data is sufficient to create a comprehensive surveillance system.[227] In *Carpenter*, the Court deemed the CSLI data comprehensive due to its ability to form "a trail of location data" that was, effectively, a "dossier of the defendant's physical movements."[228] The majority was quick to point out the unprecedented nature of CSLI data, noting that, "when *Smith* was decided in 1979, few could have imagined a society in which a phone

221. *See* Schlabach, *supra* note 212, at 680; Bodien, *supra* note 196, at 504; 18 U.S.C § 2703(b).

222. *See* Schlabach, *supra* note 212, at 680.

223. *See Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

224. *See* 18 U.S.C. § 2703(a), (d).

225. *See Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) (identifying the five factors as: (1) comprehensiveness; (2) intimacy; (3) expense; (4) retrospectivity; and (5) voluntariness); Ohm, *supra* note 156, at 370 (distilling the *Carpenter* majority into three principles: "(1) 'the deeply revealing nature' of the information; (2) 'its depth, breadth, and comprehensive reach'; and (3) 'the inescapable and automatic nature of its collection'").

226. *See Carpenter*, 138 S. Ct. at 2221.

227. *See* Uberti, *supra* note 16 ("At any given time, the way you move, the way your gait is, the way you're gazing, your pupil dilation, is giving away information to developers . . . .").

228. *Carpenter*, 138 S. Ct. at 2220.

goes wherever its owner goes, conveying to the wireless carrier . . . a detailed and comprehensive record of the person's movements."[229] The Metaverse, a similarly profound creation, collects "reams of data" from its consumers, revealing "how users interact with their surroundings."[230] This system tracks eye movements, surrounding objects in the physical reality, conversations, and more,[231] extending far beyond the mere physical movements that the CSLI data captured in *Carpenter*.[232] In fact, unless Metaverse users consent to having *all* of their conversations recorded, they are barred from talking in Meta's Horizon space.[233] If the CSLI data that tracks physical movements of a user is comprehensive,[234] then surely the data generated in the Metaverse, which tracks significantly more activity, is comprehensive as well.[235]

Second, the data collected in the Metaverse is highly intimate, as it may intrude into areas that are rooted in traditional notions of privacy, including one's home, thoughts, emotions, and private conversations.[236] The data collected by the Metaverse is so detailed that "an insurance company might obtain information that suggests a user has a health problem before the person noticed any physical changes or saw a doctor."[237] Thus, government access to Metaverse data can provide public actors with not only a window into people's homes, but also a direct view into the most intimate, personal areas of their lives.[238] This information delves far deeper into the lives of consumers than the CSLI data found in *Carpenter*.[239] Given the historically private nature of this information, unfettered government access to Metaverse data

229. *Id.* at 2217.

230. Uberti, *supra* note 16; *see* Ghi Devanur, *Metaverse: The New Frontier?*, FORBES (Jan. 26, 2022, 10:00 AM), https://www.forbes.com/sites/forbesbusinesscouncil/2022/01/26/metaverse-the-new-frontier/?sh=55793fa92671 [https://perma.cc/3BMS-6K2G].

231. *See* Uberti, *supra* note 16.

232. *See Carpenter*, 138 S. Ct. at 2220.

233. Hill, *supra* note 53.

234. *Carpenter*, 138 S. Ct. at 2220.

235. *See* Uberti, *supra* note 16.

236. *See* Furman, *supra* note 74; Coelho & Bast, *supra* note 74; Crocker, *supra* note 74, at 168, 211; *see also* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20 (discussing the Metaverse's ability to scan users' homes); Hill, *supra* note 53 (explaining how the Metaverse records user conversations); Uberti, *supra* note 16 (identifying the Metaverse's potential to harvest emotional data).

237. Uberti, *supra* note 16.

238. *See id.*

239. *Compare id.* (asserting that the technology behind the Metaverse will give companies "a unique window into users' psyches), *with Carpenter*, 138 S. Ct. at 2211 (explaining that CSLI data is merely a time-stamped record of the location of the consumer's cellphone).

would offend the United States' centuries-long commitment to the right of privacy.[240]

Third, and finally, while Metaverse users forfeit their data to Meta voluntarily, their elective participation does not necessarily bar them from the Fourth Amendment's protection against warrantless searches.[241] The Supreme Court explained this apparent contradiction in *Carpenter*, stating that CSLI data is "not truly 'shared,'" as cellphones are "'such a pervasive and insistent part of daily life' that carrying one is [necessary]."[242] Moreover, cellphones record CSLI data "by dint of [their] operation," meaning that the user need not take any action beyond "powering up" the phone to generate CSLI.[243] The same is true of the Metaverse, which collects "reams of data" from simple user interactions.[244] The collection of Metaverse data is similar in that there is no meaningful path for users to opt out once the application is in use.[245] Further, as the Metaverse continues to expand, participation may soon become "inescapable."[246] Thus, as market forces may soon compel consumers to participate in the Metaverse, without the extension of *Carpenter*, users may be deprived of their Fourth Amendment rights.[247]

Ultimately, the comprehensiveness, intimacy, and involuntariness of Metaverse data collection demands protection for users from warrantless searches.[248] By expanding *Carpenter*, the Court would effectively eliminate the applicability of the third-party doctrine to Metaverse users.[249] In doing so, the Court would ensure that the protections of the Fourth Amendment follow Metaverse users as they

---

240. *See*, *e.g.*, Teachout, *supra* note 91, at 71; Clancy, *supra* note 93.

241. *See Carpenter*, 138 S. Ct. at 2220.

242. *Id.*

243. *See id.*

244. *See* Uberti, *supra* note 16.

245. *See id.*; Ohm, *supra* note 156, at 377–78.

246. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20; John Mac Ghlionn & Brad Hamilton, *Metaverse Clothing, Travel, Plastic Surgery: Experts Predict Life in 2030*, N.Y. POST (Jan. 8, 2022, 8:08 AM), https://nypost.com/2022/01/08/experts-predict-living-in-the-metaverse-by-2030/ [https://perma.cc/5J36-FZLT] ("By 2030, 'a large proportion of people will be in the [M]etaverse in some way,' . . . ."); Ohm, *supra* note 156, at 376–78 (arguing that "inescapable" data collection is a relevant factor in extending Carpenter).

247. *See* Mac Ghlionn & Hamilton, *supra* note 246; Canny, *supra* note 60 (reporting that the value of the virtual marketplace within the Metaverse could reach between eight and thirteen trillion dollars by 2030).

248. *Cf.* HECHT-FELELLA, *supra* note 3, at 25–29 (arguing for the extension of *Carpenter* to protect body-worn technologies, smart doorbells, and internet browsing histories).

249. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (holding that "the fact that [CSLI] information is gathered by a third party does not make it any less deserving of Fourth Amendment protection").

stray "further from our base reality," and into the "new frontier."[250] Thus, despite users' voluntary forfeiture of data to a third-party organization, they would retain a reasonable expectation of privacy and therefore be safe from warrantless searches, thereby ensuring that the Fourth Amendment is not cast into the dustbin of history as the United States surges toward its new reality.[251]

2. The Potential Costs and Benefits

The immediate benefit of expanding *Carpenter* is facially apparent—the preservation of Fourth Amendment rights in the new digital world.[252] Yet, several background principles bolster the suggestion that pursuing a solution through the judiciary is the optimal approach.[253] For example, the ex post rules that courts produce may be preferable to the legislature's ex ante approach due to the difficulty of predicting technological changes.[254] Moreover, in the context of digital technologies, lawmakers are often burdened by the lack of an "easy solution," once again making courts' ex post analysis the preferable avenue.[255] Thus, as the Metaverse continues to mature, courts could utilize their interstitial decision-making approach to address new and unpredictable issues.[256]

The judicial approach, however, is not without its costs.[257] Judges frequently lack the necessary technical background to fully comprehend the vast implications of their decisions.[258] As a result, the judiciary is often "poorly suited to generate effective rules regulating criminal investigations involving new technologies" like the Metaverse.[259] In this uncertain space, judges may resort to overly formalist tests that "fail to reflect the reality of how the technologies actually work."[260] Further, in order for the Supreme Court to resolve this issue, a litigant must first suffer from a government search of his or her Metaverse data in order to have a cognizable injury for the

250. *See id.*; Devanur, *supra* note 230.

251. *See Carpenter*, 138 S. Ct. at 2223; United States v. Miller, 425 U.S. 435, 443, 446 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979); Devanur, *supra* note 230.

252. *See Carpenter*, 138 S. Ct. at 2223.

253. *See* Trepel, *supra* note 13, at 140–41.

254. *Id.* at 142.

255. *See id.* at 141, 147.

256. *See id.* at 147.

257. *See* Kerr, *The Fourth Amendment*, *supra* note 9, at 858–59; Simmons, *supra* note 11.

258. Kerr, *The Fourth Amendment*, *supra* note 9, at 858–59.

259. *See id.* at 858.

260. Simmons, *supra* note 11.

claim.[261] And, of course, before reaching the Supreme Court, different judicial circuits may arrive at different interpretations of *Carpenter*'s applicability to Metaverse technology—potentially adding a layer of confusion to the developing Fourth Amendment framework.[262] Thus, while extending the *Carpenter* decision carries many great benefits,[263] it also comes with considerable costs.[264]

B. The Legislative Solution

1. Amend the Stored Communications Act

As it currently stands, the SCA allows the government to compel the disclosure of a substantial amount of electronically stored data without first procuring a warrant.[265] Therefore, an alternative to a judicial expansion of *Carpenter* would be for Congress to amend the SCA to restrict its permissiveness, thereby enhancing the privacy of consumers.[266]

A comprehensive amendment to the SCA would create a three-tiered approach wherein: "[s]ubsection (a) . . . would protect content data from disclosure without a warrant"; "[s]ubsection (b) . . . would incorporate the mosaic theory and protect against sweeping requests for metadata"; and "[s]ubsection (c) . . . would provide limited protections against less invasive disclosures."[267] This theory seeks to dramatically enhance the privacy protections contained in the SCA by extending the warrant requirement to cover most forms of comprehensive electronic data.[268]

The first part of the amendment is simple, requiring a warrant for all disclosures of content data, not just those stored for fewer than 180 days.[269] This requirement would simultaneously bring digital content information in line with the Fourth Amendment protections

261. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

262. *See* Julian W. Smith, *Evidence of Ambiguity: The Effect of Circuit Splits on the Interpretation of Federal Criminal Law*, 16 SUFFOLK J. TRIAL & APP. ADVOC. 79, 79–81 (2011).

263. *See* Trepel, *supra* note 13, at 142.

264. *See*, *e.g.*, Kerr, *The Fourth Amendment*, *supra* note 9, at 858–59.

265. *See* Schlabach, *supra* note 212.

266. *See generally* Kerr, *Stored Communications Act*, *supra* note 210, at 1233 (advocating for Congress to amend the SCA to enhance privacy protections for consumers); Schlabach, *supra* note 212, at 697 (asserting the need for an amendment to the SCA).

267. Schlabach, *supra* note 212, at 703.

268. *Id.* at 703, 706.

269. *See id.* at 704.

afforded to physical documents while not unduly hindering government investigations.[270]

The second portion of the amendment—the implementation of the mosaic theory—would not only require a warrant for broad metadata disclosures, but it would also prohibit warrantless requests to a single provider regarding information gathered over seven or more days.[271] This alteration mirrors the comprehensiveness prong of the *Carpenter* decision, as it demonstrates an adverseness to data collection practices that occur over a lengthy period of time.[272] Thus, by bringing the SCA closer to the warrant requirement expounded in *Carpenter*, the mosaic proposition guarantees more robust privacy protections against broad government of user data, despite users' voluntary forfeiture to third-parties.[273]

Finally, the third proposal accounts for less invasive disclosures, like the session times and durations of a subscriber's phone calls.[274] Disclosures under this subsection, which are typically unintrusive and therefore not "intimate," are subject to a subpoena requirement.[275] Because these disclosures are largely unintimate and therefore lack any overarching expectation of privacy, the subpoena requirement appears appropriate in lieu of a full warrant requirement.[276]

In sum, this amendment would essentially prevent warrantless disclosures of all data collected over a period of seven or more days, and requires a warrant for any requests related to metadata and content data—regardless of whether this data meets the seven-day threshold.[277] In doing so, it pushes the SCA toward a unilateral warrant requirement for broad disclosures of electronically stored information.[278] Had this solution been in place for the Court's *Carpenter* decision, it would have prevented the warrantless acquisition of the relevant CSLI data while allowing the Court to avoid any examination of the Fourth Amendment.[279]

---

270. *Id.* at 705.

271. *Id.* at 706.

272. *See id.*; Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

273. *See* Schlabach, *supra* note 212, at 706; *Carpenter*, 138 S. Ct. at 2221.

274. *See* Schlabach, *supra* note 212, at 710.

275. *See id.*; *Carpenter*, 138 S. Ct. at 2217.

276. *See* Schlabach, *supra* note 212, at 710.

277. *Id.* at 703–04, 706.

278. *See id.* at 703.

279. *See Carpenter*, 138 S. Ct. at 2221 (acknowledging that the Stored Communications Act requires only a showing of "reasonable grounds," prompting the Court to examine the Fourth Amendment implications of the government's acquisition of CSLI data).

2. The Potential Costs and Benefits

Much like the judicial approach, a legislative approach is not without considerable costs and benefits.[280] As compared to courts, legislatures are viewed as flexible institutions capable of analyzing a wide range of input to create rules ex ante, which provide valuable notice to the public.[281] Legislatures derive their unique flexibility, in part, from the lack of stare decisis requirements on legislative activity.[282] Trusting Congress to preserve privacy protections for Metaverse users, then, ensures that the final outcome will be the malleable product of a "wide range of inputs."[283]

Yet legislatures' ex ante rulemaking method forces lawmakers to anticipate unpredictable technological developments.[284] Such a forward-looking approach may not lend itself well to the task of reining in the Metaverse, a platform still in flux.[285] Therefore, despite the valuable notice that ex ante rules may provide, legislative efforts harbor a distinct lack of responsiveness to erratic technological shifts.[286]

IV. CONCLUSION

As the United States inevitably approaches a new era of virtual reality, it is necessary to update the privacy protections afforded to consumers. The Metaverse promises to blur the lines separating the physical, virtual, and augmented realities by offering a comprehensive social platform that includes everything from workspaces to rock concerts.[287] As a result, there may soon come a point where participation in the Metaverse is nonnegotiable for a large swath of the American population.[288]

---

280. *See* Trepel, *supra* note 13, at 141, 148, 150; Kerr, *The Fourth Amendment*, *supra* note 9, at 868, 871, 875.

281. Kerr, *The Fourth Amendment*, *supra* note 9, at 868, 871, 875. *See also* Paul H. Robinson, *Fair Notice and Fair Adjudication: Two Kinds of Legality*, 154 U. PA. L. REV. 335, 376 (2005).

282. *See* Kerr, *The Fourth Amendment*, *supra* note 9, at 871.

283. *See id.* at 875.

284. Trepel, *supra* note 13, at 140.

285. *See id.* at 140, 142 (arguing that legislators often cannot anticipate technological developments and therefore pass inadequate legislation in response); Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

286. Kerr, *The Fourth Amendment*, *supra* note 9, at 868; *see* Trepel, *supra* note 13, at 140, 142.

287. *See* Meta, *The Metaverse and How We'll Build It Together – Connect 2021*, *supra* note 20.

288. *See* Mac Ghlionn & Hamilton, *supra* note 246.

In order to preserve the Fourth Amendment and protect the United States' longstanding commitment to privacy,[289] this Note contemplates two separate solutions that achieve largely similar goals: (1) an extension of the *Carpenter* doctrine, which would render the third-party doctrine inapplicable to data collected in the Metaverse; and (2) an amendment to the SCA requiring a showing of probable cause for the disclosure of large amounts of user data. While each solution has unique costs and benefits related to their judicial versus legislative nature,[290] each achieves the desired outcome: the bolstering of privacy protections for Metaverse users.

Kevin Cibak[*]

289. *See*, *e.g.*, Teachout, *supra* note 89, at 91; Clancy, *supra* note 93.

290. *See* Kerr, *The Fourth Amendment*, *supra* note 9, at 858–59; Simmons, *supra* note 11; Trepel, *supra* note 13, at 141–43, 148–49.

* J.D. Candidate, Vanderbilt University Law School, 2024; B.A., University of Pittsburgh, 2021. The Author would like to thank Professor Christopher Slobogin and the editorial staff of the *Vanderbilt Journal of Entertainment & Technology Law* for their aid and guidance in writing this Note. The Author would also like to thank his parents, James & Deirdre Cibak, and his uncle, Craig Cibak, for their unyielding support.