POST-*CARPENTER* CONFUSION TO POST-*CHATRIE* CLARITY

A. SHEA DALEY BURDETTE*

INTRODUCTION

How the Fourth Amendment's third-party doctrine applies to modern surveillance is, of course, an issue of great importance, the answer to which has sweeping implications. In less than a decade, the United State Supreme Court's decision in *Carpenter v. United States*[1] has been cited in various court opinions over two thousand times.

Because of rapidly advancing technology and ever-changing societal norms, lower courts today must routinely engage with how the third-party doctrine should be applied to numerous surveillance methods. At bottom, the Fourth Amendment's third-party doctrine in its current form was only suitable in a world where disclosing information to third-party companies was a meaningfully-voluntary choice, *i.e.*, exposures to third-party companies were always escapable and never automatic.

Today, many records reveal the privacies of life that only exist because of the digital age. Importantly, these records are created without "meaningful voluntary choice."[2] Not only have they been created without any meaningfully-voluntary choice, but individuals often disclose the information to third-party companies "without a second thought regarding whether these exposures provide the government unfettered access to intimate information."[3] Modern surveillance has required lower courts to apply the "Fourth Amendment's protections to novel surveillance practices in cases involving pole cameras, real-time location tracking, drones, smart utility meters, medical data, social media surveillance, cell site simulators, and more."[4]

In many instances, the digital age and societal norms have removed one's ability to truly choose whether to share intimate information with third-party companies. Because this lack of a meaningfully-voluntary choice is "alien to well-recognized Fourth Amendment freedoms,"[5] it is

* Assistant Professor of Law Libraries & Assistant Director of Zimmerman Law Library, University of Dayton School of Law

[1] 585 U.S. 296 (2018)

[2] ORIN S. KERR, THE DIGITAL FOURTH AMENDMENT: PRIVACY AND POLICING IN OUR ONLINE WORLD 161 (2025)

[3] *See* A. Shea Daley Burdette, *Passive Choice and the Fourth Amendment*, 62 SAN DIEGO L. REV. 799, 801 (2025) (citing Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 Harv. L. Rev. 1790, 1791–92, 1799 (2022)).

[4] Tokson, *supra* note 3, at 1811.

[5] Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

vital that the absence of choice does not nullify the protections codified by the Founder's adoption of the Fourth Amendment. The Court's third-party doctrine should be adjusted to account for today's reality. An opportunity presents itself this term—*United States v. Chatrie*.[6]

To do so, two factors currently considered within the *Katz* reasonable expectation of privacy analysis, based on the Supreme Court's decision in *Carpenter*—the inescapability and automatic nature of disclosures—should be extracted from the *Katz* "search" analysis.[7] These factors should instead be considered when analyzing whether a potential search was "unreasonable" or not by creating a new warrant exception, the *meaningfully-voluntary exposure* warrant exception.[8] The Fourth Amendment protects against "unreasonable searches" by the government without a warrant supported by probable cause.[9] Principally, "changing whether the information was inescapably or automatically exposed to a third party does not change whether the governmental action was a search; it instead changes whether the search was reasonable."[10]

I. POST-*CARPENTER* CONFUSION

In an attempt to ensure that constitutional protections continued to exist, despite advancing technology creating new surveillance methods, the Supreme Court has recognized that Fourth Amendment searches might occur in the absence of a physical intrusion into constitutionally protected areas.[11] In adopting and applying the *Katz* reasonable expectation of privacy "search" test, the Court at the time "appear[ed] to make a binary distinction between '[w]hat a person knowingly exposes to the public' and 'what he seeks to preserve as private.'"[12]

Post-*Katz* decisions held that an individual does not retain a reasonable expectation of privacy in information exposed to the public, for example when the individual has either voluntarily conveyed that information to other parties or insufficiently protected that information from the observation of others.[13]

The Court, post-*Katz*, also addressed what voluntary conveyance meant for conversations that one had with others, which the Court had previously held not to be a search in *Hoffa v. United States*[14]. In *United States v. White,*[15] the Court chose not to depart from prior precedent, continuing to find that individuals assume the risk that words shared with one might subsequently be shared with others, resulting in no reasonable expectation of privacy in conversations had with

---

[6] *See* United States v. Chatrie, __ S. Ct. __ (2026) (granting cert to 136 F.4th 100 (4th Cir. 2025)).

[7] *See* Daley Burdette, *supra* note 3, at 802–06.

[8] *See id.*

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

[10] Daley Burdette, *supra* note 3, at 819.

[11] Katz v. United States, 389 U.S. 347, 351 (1967) ("For the Fourth Amendment protects people, not places.").

[12] Daley Burdette, *supra* note 3, at 809 (quoting *Katz*, 389 U.S. at 351).

[13] *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("When [the individual] traveled over the public streets he voluntarily conveyed [particular information] to anyone who wanted to look . . . ."); *see also* California v. Ciraolo, 476 U.S. 207, 213 (1986) ("Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed.").

[14] 385 U.S. 293 (1966).

[15] 401 U.S. 745 (1971).

informants and then electronically transmitted to government officers.[16] Both pre-*Katz* and post-*Katz*, the Court held that no search occurs when words shared with one are later shared with another, because the speaker assumes the risk that the third-party will share what has been said with another.

The same was ultimately held true regarding information voluntarily shared with various third-party companies, first concerning financial records shared with a bank in *United States v. Miller*,[17] and later concerning numbers dialed that were shared with a phone company in *Smith v. Maryland*.[18] In the second case, *Smith*, the Court held that no reasonable expectation of privacy existed in phone numbers dialed from inside a home because the individual voluntarily exposed the phone numbers to the third-party company.[19] In so holding, "the Court once again pointed to its consistent holding that 'a person has no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties,'" citing its decision a few years earlier involving bank records, *Miller*, and four cases that the earlier case also relied on in making the same statement, including both *Hoffa* and *White*.[20]

The creation of the third-party doctrine based on one's risk assumption may have appropriately broadened the original *Katz* test at the time of those decisions.[21] However, the lack of a meaningfully-voluntary choice to assume the risk of such conveyances to third-party companies today has stretched the third-party doctrine to a breaking point.[22]

Ultimately, the Fourth Amendment's third-party doctrine formed because *Katz* first required the Supreme Court to consider whether an individual retained any reasonable expectation of privacy in what they voluntarily exposed to the public, including their movements while traveling on public roads, their back yards when exposed to objects flying over them, and one-on-one conversations with others.[23] The court ultimately answered each in the negative—because of the exposure to others, no reasonable expectation of privacy exists. Then, the Court relied on

---

[16] United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion) (quoting *Hoffa*, 385 U.S. at 302) (An individual verbally sharing information with another retains "'no interest legitimately protected by the Fourth Amendment . . .,' for that amendment affords no protection to 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'").

[17] 425 U.S. 435 (1976).

[18] 442 U.S. 735 (1979).

[19] 442 U.S. at 745 ("[P]etitioner voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police.").

[20] Daley Burdette, *supra* note 3, at 813 n. 88 (citations omitted).

[21] *See* Ric Simmons, *A Failed Revolution: The Muted Impact of* Jones*,* Riley*, and* Carpenter, __ WAKE FOREST L. REV. __ at 26–27 (forthcoming) (quoting *Hoffa*, 385 U.S. at 302) ("The [third-party] doctrine began innocently enough in 1966, which the Court affirmed that it had '[n]ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'").

[22] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (citations omitted) ("[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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.").

[23] *See supra* notes 13 & 15.

its decisions in cases involving private conversations with informants and undercover agents to say the same regarding exposures to third-party companies—no reasonable expectation of privacy.[24] Only two 1970s cases, *Smith* and *Miller*, involving bank records and call logs resulted in the third-party doctrine, initially understood to be a bright-line rule giving government unregulated access to information shared with third-party companies.

Until the Court's holding in *Carpenter v. United States*, the rule was simple: Any information shared with a third-party company was not protected by the Fourth Amendment. No search occurred. But even in 2018, what would have resulted from the straight-forward application of the third-party doctrine, such as the government having unfettered access to e-mails from Google or Microsoft, "[struck] most lawyers and judges [then]–[Justice Gorsuch] included–as pretty unlikely."[25]

Fortunately, the Supreme Court placed a limit on the third-party doctrine in *Carpenter*, holding that allowing the government to obtain seven days of cell site location information ("CSLI") without a warrant would be a "significant extension of [the doctrine] to a distinct category of information."[26] However, the Court's conclusion laid out a multitude of factors as relevant: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[27] The government obtaining seven days of CSLI was a Fourth Amendment search.[28]

However, the *Carpenter* Court left unclear what categories of information exposed to third-party companies the government may obtain absent a warrant based on *Smith* and *Miller*, compared to what categories of information might be protected by *Carpenter*, which requires the government to obtain a warrant. As Justice Kennedy's dissent pointed out, "the Court [did] not explain what makes something a distinct category of information."[29] The Supreme Court now has an opportunity to provide clarity that *Carpenter* lacked.

II. POST-*CHATRIE* CLARITY

The Court in "*Carpenter* changed Fourth Amendment law substantially [by] replacing a bright-line rule (where all data disclosed to a third party is unprotected) with an amorphous, flexible standard (where some data disclosed to a third party is protected . . .)."[30] Mr. Chatrie's case presents an opportunity for the Supreme Court to bring clarity to the relevancy of each *Carpenter* factor. The Court should clarify that the category of information is relevant to the "search" analysis while, on the other hand, the voluntary nature of the exposure is only relevant to the "unreasonable" analysis. This clarification produces a judicial test that adjusts "with time in a way that protects, rather than repeals, Fourth Amendment protections."[31]

---

[24] Daley Burdette, *supra* note 3, at 813.
[25] Carpenter v. United States, 585 U.S. 296, 388 (2018) (Gorsuch, J., dissenting).
[26] *Id.* at 314.
[27] *Id.* at 320.
[28] *Id.*
[29] *Id.* at 339–40 (Kennedy, J., dissenting).
[30] Tokson, *supra* note 3, at 1837.
[31] Daley Burdette, *supra* note 3, at 826.

As illustrated in Section I of this article, the third-party doctrine stems from focusing "on the *voluntary nature* of the disclosure and the defendant's assumption of the risk—in part based on what the individual knew when choosing to contract with the third party and agreeing to disclose particular information."[32] Nonetheless, a "distinction between *knowingly exposing* and *seeking to preserve as private* presumes an individual has a meaningful choice in whether to do so or not."[33]

This might explain the Court's decision in *Carpenter* to depart from its decisions in *Smith* and *Miller*, in part due to the inescapability and automatic nature of the CSLI exposure.[34] However, in doing so, the Court specified that its *Carpenter* holding was a "narrow" decision.[35] Multiple dissents took issue with the majority not explaining why the *Carpenter* holding was different than *Smith* and *Miller* and not explaining what the *Carpenter* decision meant for the continued application of *Smith* and *Miller*.[36] Justice Gorsuch's dissent stated that, post-*Carpenter*, "[a]ll we know is that historical cell-site location information (for seven days, anyway) escapes *Smith's* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned."[37]

Lower courts have continued to stay tuned for nearly a decade. In the meantime, these courts have not been able to agree on how to apply *Smith*, *Miller*, and *Carpenter* to various scenarios where individuals expose information to third-party companies, as seen by the decisions issued by the Fourth and Fifth Circuits on the geofence warrants at issue in the *Chatrie* case.

The Supreme Court now has an opportunity to provide clarity in the wake of confusion. While creating the meaningfully-voluntary exposure warrant exception will not provide a clear answer in every case, it will institute a clear process to determine such answers.

All facts outside of the inescapable and automatic nature of the disclosure to the third party should continue to be considered under the *Katz* reasonable expectation of privacy "search" test, to determine whether the government action was a search. Then, if the Court finds there to be a search, whether the disclosure to a third-party company was inescapable or automatic would determine if the particular search was "unreasonable" or not.

If the government action was a search, and the disclosure to the third-party company was either inescapable or automatic, the search would be unreasonable—the government needs a warrant, absent a separate warrant exception providing a distinct reason that the search might be considered reasonable.

By contrast, if the government action was a search, but the disclosure to the third-party company was neither inescapable nor automatic, then the search would be considered reasonable

---

[32] *Id.* at 813 (emphasis in original) (citations omitted).

[33] *Id.* at 809 (emphasis in original).

[34] *See Carpenter*, 585 U.S. at 314 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."); *id.* at 315 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI.").

[35] *Id.* at 316.

[36] *See id.* at 388 (Alito, J., dissenting) ("Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.").

[37] *Id.* at 397 (Gorsuch, J., dissenting).

because the individual voluntarily assumed the risk of said third-party exposure in a meaningful way—the government does not need a warrant.

Some circuit judges are already engaging with this proposed two-step process in their application of *Carpenter*. Therefore, adopting the meaningfully-voluntary exposure warrant exception is not only consistent with the Supreme Court's various third-party doctrine decisions, but also consistent with the way some lower courts have engaged with the third-party doctrine post-*Carpenter*. For example, in looking at the circuit split before the Court in Mr. Chatrie's case, the Fifth Circuit's *United States v. Smith* opinion and multiple Fourth Circuit *Chatrie* concurrences each identified and engaged in the two distinct analyses separate from one another—first analyzing the category of information and later engaging with the question of whether the individual voluntarily exposed said information to the third-party company.

Judge Richardson's concurrence in *Chatrie v. United States* held that no search occurred.[38] In doing so, the concurrence stated: "*Carpenter* identified two rationales that justify applying the third-party doctrine: the limited degree to which the information sought implicates privacy concerns and the voluntary exposure of that information to third parties. Both rationales apply here."[39] Judge Richardson then "[s]tart[ed] with the [private] nature of the information sought,"[40] and later concluded that Mr. "Chatrie voluntarily exposed his location information to Google by opting in to Location History."[41]

Even in reaching a different conclusion, Judge Wynn's *Chatrie* concurrence followed a similar dichotomy. Section II of the concurrence first engaged with four factors: the comprehensiveness of the data, the retrospectivity of the data, the revealing nature of the data, and the barriers to the information—how easy, cheap, and efficient the surveillance was.[42] Judge Wynn's concurrence held that "all four considerations that led *Carpenter* to conclude . . . the Government . . . invaded Carpenter's reasonable expectation of privacy' apply with equal or greater force here."[43] Then, in Section III of the concurrence, Judge Wynn analyzed the voluntariness of the exposure of information to Google.[44] Regarding this second question, the concurrence stated that "[s]haring Location History—while admittedly not wholly 'inescapable'—is not meaningfully voluntary either."[45]

Judge Berner's *Chatrie* concurrence likewise separately considered the nature of the information and the voluntariness of the exposure, using two separate headings: "Non-Anonymous Location History Data is Highly Revealing" and "*Chatrie*'s Disclosure of His Location History Data was not Sufficiently Voluntary to Defeat His Reasonable Expectation of Privacy."[46] Judge Berner's concurrence concluded that "[b]ecause non-anonymous Location

[38] United States v. Chatrie, 136 F.4th 100, 130–41 (4th Cir. 2025) (en banc) (Richardson, J., concurring).
[39] *Id.* at 138–39.
[40] *Id.* at 139 (citation omitted).
[41] *Id.* at 140 (citation omitted).
[42] *Id.* at 120–25 (Wynn, J., concurring in the judgment).
[43] *Id.* at 125 (quoting *Carpenter*, 585 U.S. at 313).
[44] *Id.* at 125–29.
[45] *Id.* at 127.
[46] *Id.* at 149–53 (Berner, J., concurring).

History data is highly revealing, the first *Carpenter* factor"—the revealing nature of the information—"weighs in favor of Chatrie."[47] Then, regarding the voluntariness of the exposure, the concurrence concluded that because "[t]he third-party doctrine concerns data that one 'knowingly share[s]" with a third party,'" in Mr. Chatrie's case, "the disclosure of th[e] data cannot be considered 'knowing'" when "users cannot determine what kind of data is being collected in the first instance."[48]

The Fifth Circuit's decision in *United States v. Smith*[49] also recognized the distinct relevancy of these two separate *Carpenter* rationales in its recent geofence warrant opinion: "The [Supreme] Court concluded [in *Carpenter*] that the criminal defendant had a 'reasonable expectation of privacy in the whole of his physical movements.' The Court then addressed the third-party doctrine, which provides that generally, 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'"[50] The Fifth Circuit held that "[g]iven the intrusiveness and ubiquity of Location History data, [the defendants] correctly contend[ed] that they [had] a 'reasonable expectation of privacy' in their respective data. Additionally, per *Carpenter*, the third-party doctrine [did] not apply."[51] The Fifth Circuit first decided that there was a reasonable expectation of privacy based on the nature of the information. It subsequently concluded that the voluntary nature of the exposure, or lack thereof, did not forfeit the individual's reasonable expectation of privacy.

While not stated in the Supreme Court's *Carpenter* decision, nor in the Fifth Circuit's opinion in *Smith*, nor in the *Chatrie* concurring opinions of Judges Richardson, Wynn, and Berner, the first analysis regarding the category of information is the only one of the two rationales that is relevant to whether a "search" occurred. The second rationale is instead relevant to determining whether the search was "unreasonable" or not.

Requiring courts to engage in two different analyses is consistent with the *Carpenter* opinion itself, which saw the voluntary exposure as a "second rationale underlying the third-party doctrine."[52] The first analysis to determine the type of information, based on the revealing nature of the information obtained as well as its depth, breadth, and comprehensive reach, goes to whether there is a reasonable expectation of privacy in that information,[53] potentially making the government conduct a search. The second analysis of the potential voluntary nature of the exposure, based on whether the exposure was neither inescapable nor automatic, goes to whether the search is unreasonable.

---

[47] *Id.* at 151.

[48] *Id.* at 153. (quoting *Carpenter*, 585 U.S. at 298).

[49] 110 F.4th 817 (5th Cir. 2024)

[50] *Id.* at 832 (citations omitted).

[51] *Id.* at 836.

[52] *Carpenter*, 585 U.S. at 315.

[53] "[T]he revealing nature of information logically impacts how likely one is to want the information to remain private." Daley Burdette, *supra* note 3, at 824 n.158 (citing Tokson, *supra* note 3, at 1801 ("The revealing nature of the information collected refers to its tendency to disclose sensitive or intimate details about an individual's life . . . . Such sensitive or intimate details are arguably at the very core of the concept of Fourth Amendment privacy.")).

Government action being a search and that search being unreasonable are each necessary conditions to trigger Fourth Amendment protections. Ultimately, moving two separate factors from the *Katz* search analysis "to instead create a warrant exception will clarify [the *Carpenter*] shift and what results from the change."[54]

It is important to ensure that inescapable and automatic disclosures to third-party companies do not erode bedrock Fourth Amendment protections to sand.[55] "In such circumstances, where an individual's subjective expectations [have] been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously [can] play no meaningful role in ascertaining . . . the scope of Fourth Amendment protection . . . ."[56] Technological advancements and changes in societal expectations make exposures today to third-party companies either inescapable or automatic. This is an influence alien to well-recognized Fourth Amendment freedoms, requiring a change to the third-party doctrine in its current form.

III. APPLYING THE *MEANINGFULLY-VOLUNTARY EXPOSURE* WARRANT EXCEPTION

Justice Gorsuch's dissenting opinion in *Carpenter* raised the question of whether the government could obtain one's emails from Google or one's DNA from 23andMe, based on the third-party doctrine, and stated that the answer to each was unclear post-*Carpenter*.[57] Recognizing the proper relevance of the individual's exposure to a third-party company under a newly recognized meaningfully-voluntary exposure warrant exception analysis provides the answers to both questions posited by Justice Gorsuch.

A. Various DNA Evidence

The government swabbing an individual's cheek for his or her DNA is considered a search.[58] However, DNA might be obtained by the government in other ways, such as when citizens submit their DNA to various ancestry databases, such as 23andMe,[59] which involves disclosure of that information to a third-party company.

While individuals have a reasonable expectation of privacy in their DNA, facts are more nuanced when it comes to the government's use of DNA databases. Often, the suspect him or herself has not provided DNA to the third-party company, such as 23andMe. Instead, a family member usually has. In those circumstances, the DNA being "searched" within the database is not the suspect's DNA. Thus, the suspect would not have standing to challenge the government

[54] Daley Burdette, *supra* note 3, at 814.

[55] *Id.* at 827 ("Correcting the doctrine by considering the inescapable and automatic nature of a third-party exposure, not as factors in the Katz 'search' analysis, but rather a question of reasonableness at the warrant exception stage ensures that inescapable and automatic third-party disclosures do not erode the Fourth Amendment bedrock to sand.").

[56] *Smith*, 442 U.S. at 740 n.5.

[57] *See Carpenter*, 585 U.S. at 388 (Gorsuch, J., dissenting).

[58] *See* Maryland v. King, 569 U.S. 435, 446 (2013).

[59] *About*, 23ANDME RESEARCH INSTITUTE, www.23andmeresearchinstitute.org [https://perma.cc/WN7J-5XB9] ("Uniting people everywhere under the common goal of improving health and deepening our understanding of DNA – the code of life.").

action nor would they have a reasonable expectation of privacy in their family member's DNA profile.

However, if the suspect has shared his or her own DNA with the DNA database, then the suspect would have both standing to challenge the government action and would retain a reasonable expectation of privacy in their DNA profile, making the government action a search. Nevertheless, the exposure of the individual's DNA to the third-party company is not an inescapable choice and does not in any way occur automatically. Thus, under the proposed meaningfully-voluntary exposure warrant exception, the government action would be seen as a reasonable search and would not be protected by the Fourth Amendment. No warrant is needed. To be sure, other scenarios exist in which disclosure of one's DNA to a third-party company would be seen as inescapable or automatic. For example, if one's DNA profile is housed within MyChart[60] from a visit to a doctor: "While some people may choose not to go to a doctor for regular checkups, doing so is widely accepted as the responsible thing to do, an inescapable part of living in today's society."[61]

Further, another potential inescapable exposure of DNA might include employers or universities requiring employees and students "to complete COVID tests in order to continue working or going to school."[62] The employees and students maintain a reasonable expectation of privacy in their DNA; thus, the government obtaining that DNA from the employer or university would be a search.[63] However, it is less clear whether the employees and students made "an escapable and active choice . . . to participate in those tests when the individuals were already enrolled or employed prior to the tests being deemed a requirement."[64]

This application of the proposed warrant exception to various methods of obtaining an individual's DNA illustrates the clear process that courts would follow to analyze whether there has been a meaningfully-voluntary exposure to a third party, to determine whether a "search" is "unreasonable" or not.

B. Information Shared with Google

While *Chatrie* specifically involves the exposure of one's location information to Google, Justice Gorsuch's dissenting opinion in *Carpenter* raised a different question: whether the government could obtain emails from Google without a warrant supported by probable cause.[65] Justice Gorsuch went on to say that if the answer is yes, then the "result [struck] most lawyers

[60] MyChart maintains patient records and is used by major medical providers such as Cleveland Clinic. *See MyChart*, CLEVELAND CLINIC, https://my.clevelandclinic.org/online-services/mychart [https://perma.cc/D97J-9NQJ]. MyChart serves over 305 million patients, including individuals in all 50 states. *MyChart is Epic!*, MYCHART, https://www.mychart.org/About [https://perma.cc/3LVF-UFJV].

[61] Daley Burdette, *supra* note 3, at 832 (citation omitted). While medical information is currently statutorily protected by the Health Insurance Portability and Accountability Act of 1996 and state laws, reliance on those laws begs the question of Fourth Amendment protection in the event those laws are amended to lessen statutory protection in the future.

[62] *Id.* at 832 (citation omitted).

[63] *See King*, 569 U.S. at 446.

[64] Daley Burdette, *supra* note 3, at 832.

[65] *Carpenter*, 585 U.S. at 388 (Gorsuch, J., dissenting).

and judges [then]—[himself] included—as pretty unlikely."[66] The answer that would result from the proposed meaningfully-voluntary exposure warrant exception is consistent with this intuition.

Individuals reasonably expect privacy in one-on-one correspondence from the view of others not part of the communication. Even in the cases that the third-party doctrine stems from involving informants and undercover officers, the disclosing party communicated directly with either the informant or undercover officer that subsequently shared that communication with another. The same is not true if the government goes to Google to obtain emails between one person and another—Google is not a participant in the communication, unless of course that other person is Google itself, such as when one emails Google support. Thus, there is a reasonable expectation of privacy in the email communications in which Google is not a party. The government action to obtain those emails should be considered a search.

However, the search of emails might become reasonable under one of the various warrant exceptions. For example, if there is an emergency that allows a search under the exigent circumstances warrant exception, or if one of the individuals consent to the search of the email communications within which he or she was a member of. In each scenario, the search would be considered reasonable.

Looking at the proposed meaningfully-voluntary exposure warrant exception, if that exposure of one's emails to Google was either automatic or inescapable, then the warrant exception would not apply. Unlike the CSLI in *Carpenter* where "cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up,"[67] emails are not created and automatically shared with Google just because a Google account exists. However, sending and receiving emails through a third-party company today is an inescapable part of being a member of modern society, similar to cell phones. For cell phones, the only real choice is which company to go through for service and what type of phone to purchase.[68] Similarly, regarding email providers, the only real choice today is which provider to sign up with to create an email address—having an email address is often how one receives invites for job interviews, how one receives their monthly bills, how one logs in to their streaming services to watch the news, etc.

Knowing the exact moment when the decision was no longer whether to have a cell phone is a difficult task, just as it is difficult to say when using email moved from being optional to necessary. What is not difficult, though, is to know that there is no meaningfully-voluntary choice today regarding whether to have an email account or not. Doing so is inescapable.

However, emails are not the only information that citizens share with Google. At issue in Mr. Chatrie's case is that Google retains precise location information over a long period of time. In *Carpenter*, the category of information appears to have made the difference.[69] Thus, based on *Carpenter*, location information is revealing enough that citizens retain a reasonable expectation

[66] *Id.*
[67] *Carpenter*, 585 U.S. at 315.
[68] *See* Daley Burdette, *supra* note 3, at 833.
[69] *Carpenter*, 585 U.S. at 314.

of privacy in, at the very least, some of the de-anonymized information, but possibly all of the location information.

Nevertheless, a search is only protected by the Fourth Amendment if the search is unreasonable. In applying the meaningfully-voluntary exposure warrant exception, the Court should ask whether the disclosure to Google was automatic or inescapable. Neither party appears to claim that the exposure was automatic in *Chatrie*. Therefore, the only question under the proposed meaningfully-voluntary exposure warrant exception would be whether the exposure was inescapable.

This essay takes no position on whether Mr. Chatrie's exposure of his location to Google was inescapable or not. As seen within the Fourth Circuit's various concurring opinions, the answer is debatable. However, that answer should be decisive. This is because "extracting [two] factors currently considered under the *Katz* reasonable expectation of privacy search analysis—inescapability and automatic nature—and moving the two factors to the proper place when asking whether the search was 'reasonable' will allow courts to clearly and correctly reapply *Katz* in third-party situations."[70]

CONCLUSION

As the Supreme Court has historically recognized, the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power.'"[71] To ensure this continues to be the case, it is imperative that the Fourth Amendment "not cease to exist simply because, in some contexts, any meaningful choice regarding whether to expose information to third parties has been subsumed."[72] Adjusting Fourth Amendment doctrine in response to advancing technology is not a new concept: "[W]hen police deploy new surveillance tools like thermal imaging devices, GPS devices, and sense-enhancing devices, the courts often adjust Fourth Amendment doctrine to increase privacy rights."[73] Technology has advanced in a way that allows the government to obtain location information in a variety of ways, as demonstrated by *Carpenter* and *Chatrie*.

Importantly, *Carpenter* separately considered the category of information and voluntary nature of the information's exposure to a third-party company in holding that the government needed a warrant in that case.[74] Although it considered both when determining whether the government action was a "search" under the *Katz* test, "[a]nalyzing a defendant's third-party disclosure as a factor under the *Katz* reasonable expectation of privacy search doctrine confuses the relevancy of the question, resulting in contradictory results without a cognizable explanation."[75]

---

[70] Daley Burdette, *supra* note 3, at 836.

[71] *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

[72] Daley Burdette, *supra* note 3, at 804.

[73] Ric Simmons, *Terry in the Age of Automated Police Officers*, 50 SETON HALL L. REV. 909, 944–45 (2020) (citing Orin S. Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 496–502 (2011)).

[74] *Carpenter*, 585 U.S. at 320.

[75] Daley Burdette, *supra* note 3, at 804.

Chatrie presents an opportunity to right the ship. The category of information analysis is relevant to asking whether a Fourth Amendment "search" occurred. The voluntary nature of exposing that information to a third-party company is relevant to determining whether a Fourth Amendment search was "unreasonable" or not. Making this clear and "[a]sking whether the third-party *meaningfully-voluntary exposure* warrant exception applies based on an individual's assumption of the risk—through an escapable and active choice—will change with time in a way that protects, rather than repeals, Fourth Amendment protections."[76]

[76] *Id.* at 826.