Wake Forest Undergraduate Law Review

Issue 1 Volume 1

Near Perfect Surveillance: Analyzing The Constitutionality of Geofence Warrants and Preparing for a Technological Future

Fritz Mezger

Wake Forest Undergraduate Law Review

Civil Law Department

Spring 2026 Volume One Issue One

Abstract

Investigative techniques bolstered by technological innovations have progressively tested the bounds of the Fourth Amendment's protection against search and seizure; recent cases have raised doubt on the constitutionality of geofence warrants. A geofence warrant compels location service providers such as Google to disclose identifying information of mobile devices that entered a specified location during a predetermined frame of interest. The emergence of geofence warrants considers the trade-off between constitutionally protected privacy pursuant to the Fourth Amendment and investigative efficiency. The Fourth Circuit Court in *United States vs. Chatrie* held that — under the premise of the Third-Party Doctrine — there is no reasonable expectation of privacy in the information collected by location service providers. In *United States vs. Smith*, however, the Fifth Circuit Court ruled that the searches were unconstitutional, warning of "near perfect surveillance." In recent years, geofence warrant requests have skyrocketed, as data shows an increase from 982 in 2018 to 11,500 in 2020. Reports from 2021 indicate that such applications constituted around a quarter of all warrants. This article first assesses the current legal situation regarding such warrants. It then posits the argument that, while parts are constitutional, geofence warrants as a whole are unconstitutional, for they contain advanced privacy searches unauthorized by the initial warrant. The article will then attempt to answer the question: how can the government write legislation that proactively accommodates technological innovations?

Table Of Contents

I. INTRODUCTION

In 1927, federal agents wiretapped the private conversations of Ray Olmstead, a suspected bootlegger during Prohibition.[1] The Supreme Court of the United States later presided over Olmstead's case, holding that due to a lack of physical trespass and seizure of material items, federal agents had not infringed upon Mr. Olmstead's Fourth Amendment protection against search and seizure.[2] In many ways, this case marked the beginning of what has become a long relationship between investigative technological innovations and privacy rights, the latest phase of which is the creation of geofence warrants. Often referred to as a reverse warrant, a geofence warrant is used when law enforcement agents do not have a clear suspect in an investigation. Thus, officers compel location service providers such as Google to release devices, in the form of anonymized data points, that entered a predesignated location during a specific time interval, from which law enforcement pares to discover suspects.[3] To find devices, Google conducts an exhaustive search of the Sensorvault, a vast repository of data containing the full location history collected on user devices that opt-in to Google's location services.[4]

The importance of privacy rights extends far beyond everyday life. The right to privacy is vital to the very structure of democracy. A system devoid of such rights crowds out the possibility for independent thought: the dynamic and subjective perspectives that are essential for a self-governing democracy.[5] Privacy lawyer and author Julia Cohen warns against this kind of "modulated democracy" where citizens "lack the ability to form and pursue meaningful agendas for human flourishing."[6] If individuals are subject to incessant surveillance, there is little room for original, subversive thought for fear of the consequences of breaking the

[1] Olmstead v. United States, 277 U.S. 438 (1928), overruled by Katz v. United States, 389 U.S. 347 (1967).
[2] *Id.*
[3] United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024).
[4] *Id.*
[5] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).
[6] *Id.*

status quo, thus rendering communities controllable, predictable, and entirely stagnant. Communities as such are highly susceptible to both sly and forthright authoritarian efforts that generate democratic backsliding due to a lack of the necessary intellectual capacity to challenge systemic norms.

This article assesses the newest phase of the interplay between investigative innovations and privacy rights. Part II will analyze the text of the Fourth Amendment, highlighting the technicalities of the Particularity Clause, while exploring relevant historical interpretations such as the Third-Party Doctrine. The importance of the court rulings in *United States v. Chatrie* (2023)[7] and *United States v. Smith (*2024),[8] as examined in Part III, proves essential to the debate surrounding reverse warrants, as the courts provide modern legal arguments on both sides. Subsequently, Part IV considers the aforementioned cases and presents a framework for how future rulings might consider the constitutionality of geofence warrants. Looking towards the future, Part V will ponder the question: how are courts to prepare for a complex investigative future, while respecting citizens' privacy rights? Ultimately, this article argues that geofence warrants, in the manner of their current usage, are unconstitutional pursuant to the Fourth Amendment because their advanced stages constitute additional searches that do not uphold the Particularity Clause. To rectify this, law enforcement must obtain further authorization to continue the reverse-warrant process after step one.

II. Text and History of the Fourth Amendment

A. *Overview and General History*

[7]Chatrie, 1 F.4th at 130
[8] United States v. Smith, 110 F. 4th 817 (Court of Appeals, 5th Circuit 2024).

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[9]

The Fourth Amendment's warrant requirement traditionally contains three primary clauses which detail a constitutionally valid warrant and search: issuance by a neutral magistrate, probable cause, and particularity.[10] The stipulation of particularity that a valid warrant must "particularly describe the place to be searched, and the persons or things to be seized" — is of central focus to this article.[11] In 1967, the Supreme Court heard *Warden v. Hayden*; the case centered around a 'hot pursuit' police entry into a house to arrest an armed robbery suspect without a warrant, which established that the Fourth Amendment protects privacy rather than physical property.[12] The Court affirmed the purpose of the particularity requirement, elaborating that the scope of a search must
be "strictly tied to and justified by" the circumstances which generated the possibility of its inception.[13] In *Marron v. United States* (1979), the Court considered just how far the boundaries of the warrant requirement extend: specifically, if officers could confiscate items not particularly listed in the initial warrant.[14] When delivering the opinion of the
Court, Justice Pierce Butler held that this doctrine is fundamentally intended to "make

[9] U.S. Const. amend. IV.
[10] *Fourth Amendment*, U.S. Const., Justia Law, https://law.justia.com/constitution/us/amendment-04/ (last visited Feb. 22, 2026).
[11] U.S. Const. amend. IV.
[12] Warden v. Hayden, 387 U.S. 294 (1967)
[13] *Id.*
[14] Marron v. United States, 275 US 192 (Supreme Court 185 AD).

general searches under them [the warrants] are impossible and prevent the seizure of one thing under a warrant describing another."[15] The articulation indicates the Fourth Amendment's preventative nature against "general searches," revealing the particularity requirement's ultimate aim: limiting officer discretion as to what is to be searched.

As it relates to personal privacy on an individual's cellular device, a key interpretive case of the Fourth Amendment came in *Riley v California* (2014).[16] On August 22, 2009, law enforcement stopped David Leon Riley for a traffic violation in San Diego, California.[17] An officer, immediately following the arrest, confiscated a cell phone from Riley's pocket.[18] Upon searching the device, the officer found repetitive text messages utilizing a term associated with a local street gang.[19] Later, at the police station, a detective further examined the digital contents, including photographs and videos, which were used to connect Riley to a shooting that had occurred weeks prior.[20] Riley moved to suppress all evidence found on his phone pursuant to his Fourth Amendment rights, but the trial court rejected this motion, and the denial was affirmed on appeal.[21] The Supreme Court then granted a writ and held that digital information stored on a cell phone was of a qualitative difference to other forms of evidence they had reviewed in past cases, therefore placing the search of Riley's phone under the Fourth Amendment.[22] Specifically, Chief Justice John Roberts, in delivering the opinion of the Court, noted how, for many Americans, cell phones hold "the privacies of life."[23] One such privacy concern is location history, which can track an individual's precise movements "down to the minute, not only around town but also within a particular building,"[24] providing an almost perfect depiction of someone's actions. The

[15] *Id.*
[16] Riley v. California, 573 US 373 (Supreme Court 2014).
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*

Fourth Amendment's fundamental purpose is to protect the "privacies of life" by ensuring that law enforcement may only intrude on an individual's privacy when a detached magistrate has approved all decisions.

B. *The Third-Party Doctrine and the Fourth Amendment*

Concerning the Fourth Amendment, the Court's property-based jurisprudence had historically required a physical trespass into a constitutionally protected area for a search to be deemed illegal. Notwithstanding, the Court in *Katz v. United States* (1967) overturned this methodology.[25] The case centered around federal agents' use of

eavesdropping devices on Charles Katz's private conversations conducted from a public telephone booth; it prompted the Court to consider whether the traditional philosophy necessitating physical intrusions into a constitutionally protected area was still valid with regard to the Fourth Amendment.[26] They reversed previous rulings, establishing that the Fourth Amendment "protects people, not places."[27] Put simply, the Court's decision in *Katz* recognized a new standard for privacy: the protection against search and seizure extended beyond locations, but protected that which one may reasonably presume to have privacy in. This decision effectively created the ensuing Katz test, which presents a twofold requirement that first assesses whether a person has "exhibited an actual (subjective) expectation of privacy," and second, if such expectation is "one that society is prepared to recognize as 'reasonable.'"[28] Evidently, searches that fail the Katz test are legally valid, while those that pass are unconstitutional pursuant to the Fourth Amendment.[29]

---

[25] Katz v. United States, 389 U.S. 347 (1967).
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

Through multiple cases, the Court has elucidated this test by clarifying the bounds of privacy expectations that society might deem reasonable in certain situations. Put simply, various rulings have examined whether an individual has a reasonable expectation of privacy in information provided to other parties, such as phone companies or banks. The prevailing consensus, articulated in *United States v. Miller* (1976), is that individuals lack the reasonable expectation of privacy detailed by *Katz* in the information they release to third parties, thus authorizing law enforcement to seize such evidence without a warrant.[30]

From 2010-2011, the FBI obtained 12,898 cell-site location information (CSLI) points on interstate robbery suspect Timothy Carpenter's phone across 127 days; Carpenter moved to suppress this data in court, but his motion was denied.[31] The Supreme Court granted a writ and heard *Carpenter v. United States* (2018), addressing whether the Third-Party Doctrine included cell-site location information gathered by the FBI.[32] The Court, applying the precedent set in *Riley*, ruled that CSLI records indeed intrude upon the reasonable expectation of privacy that individuals have "in the whole of their physical movements."[33] The Court's decision designated the CSLI-types of information collected by the government "near perfect surveillance,"[34] of the potentially pervasive implications of this data and its successors. The holding further negated the argument of Third-Party Doctrine, recognizing that the ubiquity of cell phones in quotidian life and the lack of affirmative actions on the user's part to authorize location tracking cause the *Miller* precedent to topple: "cell phone location information is not truly 'shared' as the term is normally understood."[35] In *Carpenter*, the court first recognized the evident privacy intrusion

[30] United States v. Miller, 425 US 435 (Supreme Court 1976).
[31] Carpenter v. US, 585 US 296 (Supreme Court 2017).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

caused by law enforcement's tracking of personal location as it relates to the Third-Party Doctrine.

III. The Current Legal Landscape

Before assessing the arguments in the two landmark cases concerning geofence warrants, a precise, analytical definition of the warrant process is required.

Google stores all location history in its Sensorvault database, a vast repository that assigns approximately 592 million individual accounts with a unique identification number and maintains the location history associated with each device.[36] When law enforcement, after having ascertained a geofence, compels Google to provide such location history, they follow the three-step process created by the tech giant to limit the potential for pervasive, general searches.[37] In step one, Google scrutinizes the Sensorvault to provide the police with an anonymized list of users whose location history reports them to be within the scope of the warrant.[38] A user profile at step one includes an anonymized device number, timestamp, coordinates of given location points, a confidence interval (Google aims for an average of 68% accuracy), and the source from which the location was derived (e.g., GPS or Wi-Fi)."[39] For step two, the warrant gives law enforcement full discretionary ability in that they review the provided information and urge Google to provide additional location coordinates for a list of users if deemed necessary.[40] Such additional information is unbridled by the bounds of the original geographical and temporal limits of the warrant; for any identified user, police can track movements inside and out of the geofence over a sweeping period.[41] Finally, at step three,

[36]Chatrie, 1 F.4th at 130.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*

investigators procure a list of users and force Google to de-anonymize them, typically providing names and email addresses.[42]

A. A Bank Robber and A Constitutional Warrant

On May 20, 2019, Okello Chatrie robbed a bank in Midlothian, Virginia, of 195,000 dollars in cash.[43] When Detective Joshua Hylton's initial search, reviewing surveillance footage and interviewing witnesses, failed, he turned to Google with a geofence warrant.[44] The geofence involved a 150-metre radius covering the bank, and a window of thirty minutes before and after the robbery occurred for Google to provide user location history.[45] At step one, Google provided 209 data points from 19 accounts; for step two, the list was pared to nine accounts from which law enforcement obtained 680 data points from an extended two-hour period; ultimately, Detective Hylton required information on three accounts, one of which belonged to Okello Chatrie.[46]

On September 17, 2019, a grand jury in the Eastern District of Virginia indicted Chatrie.[47] He later moved to suppress the evidence obtained, arguing the geofence warrant violated his Fourth Amendment rights.[48] The district court denied this motion on the premise of the good-faith exception.[49] This exception allows for the admission of evidence seized in violation of the Fourth Amendment, given that it was collected by officers who reasonably believed their actions to be lawful.[50] The court further refused to address whether the warrant did indeed violate the Fourth Amendment.[51]

---

[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] United States v. Leon, 468 US 897 (Supreme Court 1984).
[51] Chatrie, 1 F.4th at 130.

The Court of Appeals for the Fourth Circuit ruled again against Chatrie, considering two primary bases for their decision: the nature of the information sought and the voluntary exposure of this nature.[52] The court declined to extend the *Carpenter* decision (that tracking an individual's location constitutes a Fourth Amendment search) to Chatrie, for the two hours of his location history were far from an "all-encompassing record of [Chatrie's] whereabouts … provid[ing] an intimate window into [his] person[al] life."[53] Tracking one trip that Chatrie took was therefore much less revealing than searches that had been considered in the past, such as that of *Carpenter*. The court asserted that the information obtained was not sufficient for police to secure a picture of Chatrie's life: that which Chatrie "does repeatedly, what he does not do, and what he does ensemble."[54] Furthermore, the court evaluated the voluntary nature of Google's location history process, implicating the Third-Party Doctrine. By default, Google's location history is off; it requires an affirmative act by the user to activate the tracking and storing of one's information.[55] In fact, Google provides notice of the nature of this setting before it allows a user to enable location history by prompting the user with text that informs them about what the tracking does with the information and their ability to change the data.[56] Per the Court of Appeals for the Fourth Circuit, the location history reviewed in *Chatrie* was not nearly as pervasive and socially necessitated as that of *Carpenter*, for the activation of location history is ultimately unnecessary, and Chatrie voluntarily decided to opt in; thus, he had no reasonable expectation of privacy in the information.[57]

---

[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*

B. A Postage Robber and An Unconstitutional Warrant

On February 5, 2018, three individuals robbed United States Postal Service Driver Sylvester Cobbs, assaulting him and stealing $60,706 from mail bags that contained cash receipts.[58] Postal Inspector Steven Matthews began his investigation three days after the occurrence; he obtained surveillance footage that included what he believed to be one of the assailants utilizing a cell phone.[59] By November of 2018, Inspector Todd Matney and Steven Matthews testified that they had much difficulty identifying the individuals involved in the robbery, which is when they turned to a geofence warrant to locate potential suspects.[60] In response to the warrant, Google provided the investigators with a list of eleven accounts located within the approximately 378,278 square meter area in one hour, from five to six pm on the night of the incident.[61] Through the next two steps, inspectors Matney and Matthews paired the list to three accounts that were then identified as belonging to Jamarr Smith, Gilbert McThunel, and a third, deemed irrelevant by the investigators.[62] Later, after conducting further searches on Smith and McThunel, law enforcement also identified Thomas Iroko Ayodele as a suspect.[63]

Smith, McThunel, and Ayodele were indicted on October 27, 2021.[64] The district court denied their motion to suppress on the grounds of an intrusion into their privacy and violation of the Fourth Amendment. However, after expert testimony from the prosecution, all three individuals were found guilty.[65]

In the Fifth Circuit Court of Appeals' ruling that the geofence warrant was indeed a Fourth Amendment search, the court addressed two main topics: a reasonable expectation of

[58] Smith, 110 F.4th 817.
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

privacy and general constitutionality. Citing the ruling in *Carpenter* and referring to previous decisions, the court reaffirmed that individuals have "a reasonable expectation of privacy in the whole of their physical movements," not to be infringed upon by investigative searches without a warrant.[66] The court disagreed with the application of the Third-Party Doctrine, which holds that one gives up their right to privacy by voluntarily releasing information. Instead, they warned of the "potential intrusiveness of even a snapshot of precise location data," which often reveals an individual's most personal orientations at the "click of a button."[67] This location tracking easily follows people into the spaces that they regard as the "most private and intimate," such as a house or place of worship.[68] Because the court deemed the information afforded to Google "hardly informed, and, in many instances, … not even voluntary," they declined to implement the Third-Party Doctrine.[69] The Fifth Circuit Court then considered the general constitutionality of these warrants, finding them akin to the "general warrants" that the amendment originally sought to eliminate; this is because law enforcement, when requesting a geofence warrant, "have no idea who they are looking for," and only a brief snapshot where a suspect might turn up.[70] In sum, the court in *Smith* reiterated the dangers of searching location tracking information, ruling that the use of geofence warrants was unconstitutional, upholding the privacy standard set in *Carpenter.*

IV. The (Un)Constitutionality of Geofence Warrants

This section will posit an argument for the unconstitutionality of geofence warrants founded in their inherent structure. This article holds that the anonymized list of users, which constitutes the first step of a geofence warrant, is constitutional, but that such constitutionality

[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*

dissipates at the second and third steps. It will also address other notable topics related to geofence warrants, namely, *Chatrie*'s arguments of the Third-Party Doctrine and the good faith exception.

A. *Primary Discussions*

The particularity requirement of the Fourth Amendment necessitates that a valid warrant must "particularly [describe] the place to be searched, and the persons or things to be seized."[71] Per the Court in *Marron*'s relevant interpretation, this clause primarily aims to limit officer discretion in what is to be searched.[72]

At its first step, a geofence warrant is constitutionally permissible because the initial procurement of data is limited to an anonymized list of users within a strict location and time frame. As elucidated in *Chatrie*, this phase lies on the distinction between raw location data and identifiable accounts.[73] This distinction provides the locations of users within the specified window, but presents them in a manner that makes it impossible for the direct identification of an individual. Indeed, this nuance creates a stark contrast with the expansive CSLI information obtained in *Carpenter*,[74] for it is not only limited in scope but in the traceability of the users involved. However — regarding the framework established in *Katz* — the court has maintained that there is yet a reasonable expectation of privacy in one's precise, personal location history, for it often reveals incredibly personal affiliations.[75] Therefore, the privacy intrusion in step one is minimized to the extent that it limits officer discretion towards the desired information, as it is effectively controlled by a warrant issued by a detached magistrate. The "things to be seized"

[71] U.S. Const. amend. IV.
[72] Marron, 275 U.S. 192.
[73] Chatrie, 1 F.4th at 130.
[74] Carpenter, 138 S. Ct. 2206.
[75] Smith, 110 F.4th 817.

particularly described by the warrant, which rendered the initiation of the search possible, are thus only in compliance with the particularity in step one.[76]

At steps two and three, such constitutional permissibility fails for two primary reasons: the undue discretion afforded to law enforcement and shortcomings of the *Katz* standard.

As established by the court in *Johnson v. United States* (1948), the Fourth Amendment's protection of privacy subsists not in making confidential realms entirely unreachable by investigators.[77] Instead, it requires that the "inferences which reasonable men draw from evidence" to intrude upon an individual's privacy must "be drawn by a neutral and detached magistrate," rather than law enforcement officers.[78] Put simply, the court in *Johnson* made plain that the Fourth Amendment is meant not to stop investigators entirely, but to limit their discretion regarding what is to be seized, placing this power in the hands of a warrant that has been issued by a judge. Evidently, when analyzing which users to select for further examination in a geofence warrant, law enforcement has the ability to make, validate, and act upon their own inferences, though acting only upon one warrant granted by a judge. Awarding this discerning power to officers is constitutionally unreasonable. Under one geofence warrant, law enforcement essentially conducts three different searches: of the specified window (step one), of a specific user's location (step two), and finally, of a user's personal account information (step three). These three searches are all loosely tied together and authorized by a warrant only particularly describing the evidence to be seized in step one, placing judgment in the hands of officers rather than a judge. In brief, when officers conduct the advanced privacy searches, which the second

[76] U.S. Const. amend. IV.
[77] Johnson v. United States, 333 US 10 (Supreme Court 329 AD).
[78] *Id.*

and third steps of a geofence warrant consist of, they act in a manner founded on the inferences drawn not by a detached magistrate but by an officer.

Furthermore, it is the contention of this article that the advanced steps of a geofence warrant satisfy the *Katz* test, rendering them unconstitutional. Made brief, the *Katz* test is intended to determine whether any government surveillance constitutes a Fourth Amendment search, enunciating the principle that the amendment protects "people, not places."[79] The test presents two questions: whether an individual exhibited a reasonable expectation of privacy, and if this expectation was one that society might recognize as reasonable.[80]

Under the premise of this test, the second and third steps of a geofence warrant are further deemed unconstitutional: there is indeed a reasonable expectation of privacy, exhibited by an individual and recognized by society, in one's precise location, which is intruded upon by geofence warrants. As demonstrated by the court in *Smith*, there is a foundational recognition of one's reasonable expectation "of privacy in the whole of their physical movements."[81] In various cases, the court has further maintained the notion that the modern cell phone often contains "the privacies of life" for the American people.[82] Assuredly, this constitutes a significant privacy interest for many individuals, as even a small window of exact location data may reveal to law enforcement the most personally intimate places, affiliations, and interests of an individual.[83]

In *Kyllo v United States* (2001), the Court deliberated on a case of law enforcement officers utilizing the then novel technology of thermal imaging to collect evidence on a suspect in his house.[84] The Court deemed it unconstitutional under the Fourth Amendment, specifically

---

[79] Katz, 389 U.S. 347.
[80] *Id.*
[81] Smith, 110 F.4th 817.
[82] Riley v. California, 573 U.S. 373.
[83] Smith, 110 F.4th 817.
[84] Kyllo v. United States, 533 US 27 (Supreme Court 2001).

noting information that gave police an insight into a constitutionally protected area that would not have been otherwise possible without a physical intrusion in their reasoning.[85] Granted, law enforcement gains a relatively limited view of the home when comparing geofence warrant searches to the thermal imaging seen in *Kyllo*. Even so, investigators nonetheless gain information — that is, those locations and affiliations which are the most intimate[86] — from precise, personal location history, information that would be impossible to obtain if not for a physical infringement. Law enforcement is further able to make deductions about those places where an individual exercises their most personal affiliations, for example, the "abortion clinic, AIDS treatment center … mosque, synagogue, or church"[87] among many other possibilities. These deductions concerning the most personal information would only otherwise be possible with significant physical action concerning an individual's personal affiliations. Made brief, the ensuing steps of a geofence warrant are akin to the warrantless, "general, exploratory rummaging"[88] that the Fourth Amendment was originally intended to prevent, and therefore unconstitutional.

B. *Secondary Discussions*

In the present examination of the apparent unconstitutionality of geofence warrants, the most common argument to this contention of this article must be addressed: the application of the Third-Party Doctrine from the Court in *Chatrie*. For reference, the Court held that because Okello Chatrie's decision to opt in to Google's location history was seemingly voluntary, he had no reasonable expectation in his location information as it was freely lent to a third party.[89] Be that as it may, the Fourth Circuit's assertion of voluntary agreement comes into question when

[85] *Id.*
[86] Smith, 110 F.4th 817.
[87] Haley Amster & Brett Diehl, *Against Geofences*, 74 Stan. L. Rev. 385 (2022).
[88] Smith, 110 F.4th 817.
[89] Chatrie, 1 F.4th at 130.

weighed against the common mental state of individuals when they make the aforementioned decision.

As George Washington Law Professor and privacy expert Daniel Solove contends, there are four main reasons why this consent may in fact be involuntarily given: one, people do not read privacy agreements; two, if they read the agreements, they do not understand them; three, if people have the two former abilities, they often lack the background information required to make an informed choice; four, if an individual has all such capabilities, their rational choice may still be influenced by many decision-making factors such as the framing of choices.[90] Solove continues, noting how "bounded rationality," the human inability to apply knowledge to complex situations, often prevents rational decisions.[91] The choice one makes when considering their privacy is not formed abstractly, but in the context of the world in which they exist.[92] This reality consists of mental processing errors and judgment mistakes that indeed make it sufficient to negate the *Chatrie* court's affirmation of voluntary agreement.

The court in *Smith*, moreover, indicates how such opt-in systems "may not even be voluntary" due to location tracking requests that do not clearly articulate the full situation, promising "app optimization" in return for an individual's location history to be stored by Google.[93] These misleading promises of "app optimization" often do not reflect the full pervasiveness of location tracking. Thus, the *Chatrie* court's reliance on voluntary consent is cast into doubt by the not-uncommon circumstance that people lack the necessary information to apply their knowledge and provide a wholly informed and voluntary decision.

---

[90] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013).
[91] *Id.*
[92] *Id.*
[93] Smith, 110 F.4th 817.

It is further important to note recent applications of the good-faith exception to justify the validity of evidence obtained under a geofence warrant, founded in the Court's ruling on *United States v. Leon* (1984).[94] In *Leon,* police obtained and acted upon a warrant that was later deemed invalid for an insufficiency of probable cause, meaning law enforcement technically seized evidence illegally.[95] When *Leon* reached the Supreme Court, the justices established the good-faith exception.[96] At its essence, the exception protects evidence seized in violation of the Fourth Amendment and permits its admission in trial, provided the information was collected by officers who reasonably believed themselves to be acting lawfully.[97] Appellants often argue for the implementation of the circumstances in *Leon* where the good-faith exception does not apply amidst a heap of denials to suppress evidence obtained by geofence warrants.[98] In invoking this for geofence warrants, as outlined in *Smith,* courts have recently relied on the justification that, as long as officers act in reasonable accordance with the extent of their knowledge in obtaining the warrant and collecting information, the good-faith exception still applies.[99] This application takes into account officers' circumstances and relies on the novelty of the geofence warrants, as the Supreme Court has yet to establish a clear precedent. The existing application hinges on the fact that geofence warrants are an emerging technology, a status that will soon fade away. While legally valid, the rationale cannot stand the test of time, which places incredible importance on the Supreme Court's decision on *Chatrie.* The Court must articulate a definitive answer to the good-faith exception as it pertains to geofence warrants to plot a clear future for the way that law enforcement handles evidence collected by such warrants.

---

[94] United States v. Leon, 468 US 897 (Supreme Court 1984).
[95] *Id*.
[96] *Id.*
[97] *Id.*
[98] Smith, 110 F.4th 817.
[99] *Id*.

V. Preparing for a Technological Future

So, what are the courts to do? Technological innovations offer no promises of future curtailment, and, in many ways, they must not. If not for forensic evidence inventions such as DNA and fingerprint analysis, hundreds of criminal cases may have gone unsolved.[100] Even so, the *Katz* and *Carpenter* decisions make plain an interplay between investigative efficiency and constitutional privacy rights. The nature of the law necessitates that this line, which dictates the interchange, is ever-changing to accommodate new inventions or restrict them in the name of privacy.

The objective then is to understand this line's adjustment: how courts contemplate technological change. To address this, Stanford Law Professor Orin Kerr posits the Equilibrium-Adjustment theory in his publication *The Digital Fourth Amendment: Privacy and Policing in Our Online World*.[101] Per Kerr, when a new technological efficiency "disrupts the function of the old rule," courts ought to reform doctrine so that the function of the old rule is maintained "in the world of new facts."[102] This reactionary posture aligns with the idea of sociological jurisprudence, which maintains that the social effects of legal doctrines and practices should inform the application of the law.[103] By looking at the impact that new surveillance techniques have on the "privacies of life,"[104] courts can more effectively adjust the law to protect the independent thought necessary for a self-governing democracy.

How this line must be adjusted for geofence warrants, and for future technology to come, is for the Supreme Court to consider in *Chatrie*. This issue is of special urgency, as, from January

---

[100] Joseph Peterson et al., *The Role and Impact of Forensic Evidence in the Criminal Justice Process*.
[101] Orin S. Kerr, The Digital Fourth Amendment: Privacy and Policing in Our Online World (2025).
[102] *Id.*
[103] E. F. Albertsworth, *Program of Sociological Jurisprudence*, 8 American Bar Association Journal 393 (1922).
[104] Riley v. California, 573 US 373 (Supreme Court 2014).

to June of 2025, Google received almost 290,000 requests for geofence warrants, implicating around 665,000 individual, personal, and most importantly, private location accounts.[105] Considering there is a 68% chance that a user is indeed within the coordinates provided by Google,[106] there could potentially be up to 212,000 people whose location history records them to be somewhere where they were not.

Along with geofence warrants, future courts will have to evaluate how artificial intelligence might interact with surveillance.[107] Recent reports reveal a lump sum of 30 million dollars paid to Palantir by the United States Immigration and Customs Enforcement Agency for an artificial intelligence-driven surveillance system delivering the "near real-time visibility" of individuals.[108] Future rulings must walk the line between enabling growth and adhering to the Fourth Amendment, striking a balance between upholding privacy standards and providing for technological innovations.

VI. Conclusion

Considering their recent utilization, geofence warrants are unconstitutional because their advanced stages constitute searches of private information not particularly described by the warrant that rendered the search possible. Drawing upon the modern privacy jurisprudence as asserted in *Riley* and *Carpenter* and the framework established in *Katz*, these warrants create an unconstitutional window into an individual's intimate life that would have been highly unlikely if not for a physical trespass. The warrant further affords law enforcement discretion in excess of

---

[105] *Requests for User Information – Google Transparency Report*, https://transparencyreport.google.com/user-data/overview?hl=en (last visited Mar. 15, 2026).
[106] Chatrie, 1 F.4th at 130.
[107] While artificial intelligence-based forms of surveillance are outside the scope of this article's discussion regarding geofence warrants, they represent the next logical step in the "near perfect surveillance" warned about in *Carpenter. See* Carpenter v. US, *supra* note 30.
[108] Rosemarie Ho, *ICE Just Ordered $30 Million Worth of New Technology from Palantir to Track Immigrants*, Business Insider, https://www.businessinsider.com/ice-palantir-new-technology-30-million-visa-overstays-self-deportation-2025-4 (last visited Mar. 15, 2026).

that which the Fourth Amendment permits, as it is ultimately the judgment of an officer to select what accounts will be further investigated.

The implications of this are substantial. As law enforcement continues to rely on massive stores of location data, the deeply intimate aspects of an individual's life are to continue and if the power to expose an individual's risk. If the status quo is permitted to privacy is vested in an investigator's decision, society may eventually come to function as a "modulated democracy" in which the liberal thought that free society necessitates is oppressed by incessant and ubiquitous surveillance.[109] Citizens, in fear of the revelation of their precise location history by law enforcement, may be hesitant to travel to those most personal locations where their identity and dynamism are best expressed and developed. In the present case, legislation proves far too inefficient in responding to a "world of new facts,"[110] which places special importance on how the Court interprets the application of the Fourth Amendment regarding geofence warrants. To preserve an individual's constitutional protections, the Court must act swiftly in enforcing a requirement for additional authorization to progress a geofence warrant.

[109] Cohen, *supra* note 5.
[110] Orin S. Kerr, The Digital Fourth Amendment: Privacy and Policing in Our Online World (2025).