Blindly Looking Everywhere:
How Reverse Search Warrants Affect the Fourth Amendment

Daniel Murphy

While the efforts of courts and their officials to bring the guilty to punishment are praiseworthy, they are not to be aided by sacrificing the great fundamental rights secured by the Constitution.
- Supreme Court Justice William R. Day

Introduction

Modern technology has become intertwined with daily life, allowing for information to be readily accessible at a moment's notice. As the capabilities of technology grow, people have also begun using technology for more personal interests. However, individuals are not the only ones using this technology. From app developers to giants like Google, tech companies are recording mass amounts of data, effectively capturing highly intimate details of their users' private lives. This recording can be seen in many different areas: when using cellphone apps to track fitness goals, searching the internet for answers about an odd bump on their leg, or mindlessly scrolling through videos on the computer. Each of these instances provide a nugget of information to companies that, over time, provides them with a deep insight into who the user is, what their interests are, where they live, common routes to work, medical concerns, and much more.

Law enforcement has begun to tap into these sources via an unorthodox search methodology which does not seek evidence. Instead, they look to seize the information of an individual by linking them to certain details of an investigation. These searches are conducted as "reverse search warrants," of which there are two primary kinds: geofence and keyword. Geofence warrants seek the information of users based on the geolocation of all devices within a specified area and timeframe - effectively drawing a fence around an area of search. Keyword warrants seize from a search engine company the information of all users whose queries contained specific word(s) within a timeframe.

This raises constitutional issues because law enforcement is gaining access to a wide range of information without specifying smaller areas by which to restrict their search. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and ***particularly*** describing the place to be searched, and the persons or things to be seized [emphasis added]."[1] As such, law enforcement's access to information through reverse warrants has caused concerns over whether Fourth Amendment protections might apply on the grounds that reverse search warrants fail to meet the amendment's "particularity requirement" - referencing the clause which requires the language of a warrant to be "particularly describing." To understand these issues, this paper will first look at the technological side: what information law enforcement gains when applying reverse search warrants, and what information is collected and stored by three major areas of relevance within tech. Then, the legal side will explore how interpretations of the Fourth Amendment have defined the role of technology in search warrants to date: the history of the Fourth Amendment with emphasis upon major cases that define current interpretations, tools needed to address adjacent technology, and how reverse warrants are generally impacted as a result. Finally, the impact from synthesizing technology and the Fourth Amendment will be analyzed.

Some scholars, such as Orin Kerr, believe that there are no particularity issues with reverse warrants because these queries are not searches under the Fourth Amendment.[2] They say that because the data being searched belongs to the company and not the target, the target has no expectation of privacy.[3] However, we believe that because the involved location data maps

[1] U.S. Const. amend. IV.

[2] Kerr, O. (2022) The fourth amendment and geofence warrants: A critical look at United States v. Chatrie, Reason. Available at: https://reason.com/volokh/2022/03/11/the-fourth-amendment-and-geofence-warrants-a-critical-look-at-united-states-v-chatrie/ (Accessed: 02 May 2024).

[3] *Ibid.*

moderately closely to that of the revealing location data discussed in Carpenter v. United States, then geofence warrants suffice as Fourth Amendment searches.[4] Additionally, Justice Sotomayor's concurrence from United States v. Jones suggests that voluntarily handing information over to a company does not automatically bar an expectation of privacy.[5] As such, this paper will not be discussing the matter further.

I. Technological Background

Within the past few years, tech businesses' tracking technology has become increasingly imbedded and invasive in our daily lives; apps on our cellphones suggest certain videos by recording our online viewing habits, products we just searched seconds prior are advertised to us, and even our maps are suggesting a favorite coffee shop on the way home from work. Each of these details may seem small, but they represent facets of our lives and, when viewed together, the composite becomes recognizable as a unique individual. This amalgamation can identify highly personal information such as medical issues, political or religious views. This section of the paper will be discussing how these issues materialize and impact the following three highly relevant areas of the technology market: app developers, Google, and network service providers.

These fragments of identifying personal information, stored in massive databases, can create misleading results when used for unintended purposes. This repository is not created with the intent to pinpoint, with legal accuracy, particular individuals, but rather efficiently pair ad space with consumers most likely to purchase a product. In essence, querying these databases for user information would effectively require searching every user unless qualifiers are applied to narrow the search.

While tracking technology can be accurate, details considered unnecessary for the intended purposes of the dataset can lead to erroneous conclusions when misemployed. Because of the collection methodologies employed by businesses to obtain and use data from consumers, accommodations for incompleteness in the information are irrelevant to advertisers' ability to display semi-relevant ads. Most people notice that after searching for an item, they are inundated with ads that range in relevance to their search. This process happens in mere milliseconds of an individual opening a webpage: the webpage has specific slots for ads, many of which are shown to a single user on a single occasion (impression). The slots are populated via a real time bidding system determining the highest paying advertisers and the relevancy of their ad to both scraped user data and other data in possession of the company.[6] Though advertisers are looking for the most accurate information possible, they only want the fragments most apposite to them, for example "if the information tells a particular retail advertiser that the user had previously browsed that retailer's website but did not complete a sale, then that retailer may be willing to pay a premium for the particular impression."[7] Much of this information can be and is fragmentary, making it inappropriate for searches by law enforcement. A search warrant applied to this data could easily result in inaccurate evidence or misleading information.

Many people are unaware of how much personal information companies can access about individuals and how that information is being used. While this paper by no means intends to claim that ignorance is a valid excuse, there is a very common issue of under-communication from

[4] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018)
[5] United States v. Jones, 565 U.S. 400 (2012)
[6] United States v. Google LLC, No. 23 Civ. 00108 (E.D.VA Jan. 24, 2023).
[7] *Ibid*.

companies to their customers. Explanations of what data is being collected tend to be buried deep in tortuous web pages. Knowledge of personal information usage is even harder to ascertain. Even those who are aware that personal information collected is "being sold" are usually unaware of who has collected it, to whom the information is sold, and for what purposes.

A. How Reverse Search Warrants Are Applied

Reverse searches require sifting through immense amounts of data, much of which is highly revealing information about individuals garnered from their search queries and automatic tracking of their travels. It is not challenging to envision a search query or navigation that, without full context, could look suspicious to an observer with motivated perception or reasoning: contraceptives or early parental advice, going to a Planned Parenthood, finding directions to an address, unwittingly walking nearby an active crime scene, or searching highly contentious political issues. These databases store colossal amounts of identifying information generally inaccessible to anyone but the company who owns the database.

Under the umbrella of reverse search warrants, there are geofence warrants and reverse keyword warrants. Geofence warrants are used by United States law enforcement to identify suspects within a specific geolocation and window of time.[8] These warrants create a dragnet of sorts where authorities first provide a location and time of interest when designing their warrant.[9] If the warrant is approved, said information is then used to sift through a company's database for matches attached to user data.[10]

Reverse keyword warrants use the same dragnet approach as geofence warrants but address search engine queries. These warrants compel companies to search their databases for any data responsive to search terms ("key words") identified in the warrant.[11]

A wide variety of companies such as Google, iRobot, Samsung, Starlink and Verizon collect user information. Google, in particular, tracks information from smartphones that have Google Maps installed, and from Google Search on any type of device. Google has built robust and intricate databases tracking and recording the user's movements and searches. This information is intended to be used only by Google for their own marketing and analytics.[12] Google appears to be the first and most popular choice by officers for searches, presumably because Google Search maintains the largest market share for search engines in the United States and thus would have the highest likelihood of holding salient information.[13] Depending on the type of reverse search warrant, this could include every online search term regardless of the users' intentions, or every person whose device might have been in a particular location.

B. Law Enforcement Collections

---

[8] *Geofence Warrant Primer* (2022) *NACDL Geofence Primer*. Available at: https://www.nacdl.org/getattachment/816437c7-8943-425c-9b3b-4faf7da24bba/nacdl-geofence-primer.pdf (Accessed: 24 January 2024).

[9] *Ibid.*

[10] *Ibid.*

[11] *Reverse search warrants* (no date) *NACDL*. Available at: https://www.nacdl.org/Landing/Reverse-Search-Warrants (Accessed: 24 January 2024).

[12] *Manage your location history* (2024) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3118687?hl=en (Accessed: 17 January 2024).

[13] *Search engine market share worldwide* (2024) *StatCounter Global Stats*. Available at: https://gs.statcounter.com/search-engine-market-share (Accessed: 05 February 2024).

When using reverse search warrants, law enforcement seeks to obtain identifying information regarding an unknown suspect. Law enforcement can obtain this identifying information from several potential sources, assuming the perpetrator owned either: a powered-on cell phone that was on their person at the time of the crime, or a computer with which online search engine queries could be made. The information comes from services or products such as Google Search, Google Maps, third-party smartphone apps, or network providers, all of whom can collect data on their users. Though varied, the information that law enforcement typically receives are full names, phone numbers and physical addresses among other information.[14] IP addresses of users' devices are also collected, though typically only when the data originated from computers.[15]

When investigating a crime, these discrete units of personal information are enticing to law enforcement as they may identify individuals who were present at the time of the crime or identify a perpetrator through evidence of premeditation via an online search that matches to a specific detail of the crime before it was committed. Those individuals whose movements and details align to facts identified in a crime can then be investigated under suspicion of wrongdoing. However, officers often have no identified suspects, only a hope that the perpetrator will have created a digital footprint before law enforcement requests a reverse warrant. Law enforcement lacks the ability to demonstrate that a database at least partially created for advertising purposes will likely contain evidence of the crime.

The data collection process on the part of services like Google, third-party apps, and network providers is complex and will be discussed later, but law enforcement seeks data already collected by these companies. As historically seen in cases using reverse search warrants, law enforcement tends to start with broad parameters defined in their search warrant, seeking information such as each user's full name, date of birth, email address, physical address, phone number, and IP address.[16] Broad productions are usually denied by companies like Google due to preexisting privacy and user agreements. Many companies instead determine a procedure for handling reverse search warrants and review the search terms, resulting in law enforcement refining their warrant applications to make cooperation easier. These refinements typically identify a window of time during which all devices are searched by either their geolocation coordinates or a specific online search query. Depending on the company in question, there can be various steps law enforcement must follow, including submitting subsequent warrants. Often, law enforcement is given anonymized data and must obtain new warrants to de-anonymize said data. From successfully applied search warrants, however, law enforcement can receive a wide range of user information. This may include the data of people completely unrelated to the investigation or potentially related; intimate or otherwise.

The next three sections will focus on the groups that collect personal identifying information: app developers, Google, and network service providers. These three represent the largest and most common groups scraping personal information. To date, some of these sources have scarcely seen reverse search warrants issued by law enforcement, however there is a high

[14] *In re Search Warrant Application for Geofence Location Data Stored At Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020).

[15] For technical reasons involving Network Address Translators, the IP address of a phone is often not useful, *see* P. SRISURESH & K. EGEVANG, TRADITIONAL IP NETWORK ADDRESS TRANSLATOR (RFC 3022) (2001), https://tools.ietf.org/pdf/rfc3022.pdf [https://perma.cc/QU4K-WFJH] [hereinafter RFC 3022] (explaining network address translators).

[16] Application for Search Warrant (Minn. Hennepin Cnty. Ct. Feb. 1, 2017), https://www.documentcloud.org/documents/3519211-Edina-Police-Google-Search-Warrant-Redacted.html.

likelihood this will change considering the information that is at stake.

1. App Developers

a. The Variance in Data that App Developers Collect

There is currently little legal regulation on what app developers can collect and what they can do with collected information, resulting in datasets varying wildly in size, purpose, and especially accuracy. Currently in the United States, the only major regulations for consumer data and privacy are state-level such as the California Consumer Privacy Act (CCPA), and a combination of overly specific[17] and vague rules such as the Federal Trade Commission (FTC) verbiage holding companies responsible who are found to be misleading consumers via "deceptive practices."[18] The Federal Government draws opaque, seemingly contradictory distinctions between types of personal information: highly accessible, unregulated data classified as personally identifiable information (PII) which confusingly includes as name, birthday, driver's license number, address, and some kinds of regulated information, and then the less accessible information, personal information (PI), covering IP address, contact information, voting records and more. PII contains highly revealing information that directly connects an individual, yet even the CCPA does not halt collection and use of PII; rather, it regulates when businesses in California can use certain data and provides California residents with more control over their information. Contributing to this variability is the operating system of the device and the permissions an app has been granted — iPhones control and protect user information from app access differently than Androids.

Apple controls all third-party apps on the Apple App Store by forcing conformity to Apple's provided standards, and controlling which apps are allowed to be on the Apple App Store.[19] An iPhone's architecture also helps safeguard user information by preventing apps from accessing the phone's operating system files, which are responsible for network connections, handling applications, memory management and more. However, users can control app access via general user-side privacy settings, and by extension data collection, to varying data such as activity across other companies' apps and websites (e.g. health app information or web browsing history)

[17] HIPAA protecting only medical records, financial privacy under the Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act), Children's Online Privacy Protection Act (COPPA) which does as the name implies; none of this is to take away nor admonish the FTC and similar governmental efforts for privacy, rather that these acts should only be the beginning of greater reform.

[18] A bill has been proposed that would provide new protections, however it has not yet been passed. Lima-Strong, C. (2024) *This is the most consequential technology in America - The Washington Post*, *New York Times*. Available at: https://www.washingtonpost.com/technology/2024/04/09/most-important-app-youtube/?pwapi_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZWFzb24iOiJnaWZ0IiwibmJmIjoxNzEyNjM1MjAwLCJpc3MiOiJzdWJzY3JpcHRpb25zIiwiZXhwIjoxNzE0MDE3NTk5LCJpYXQiOjE3MTI2MzUyMDAsImp0aSI6IjE2NjcwYWQ5LTIwODEtNDRkMS04YzU2LTFmNGNmZWQ3MDY1NSIsInVybCI6Imh0dHBzOi8vd3d3Lndhc2hpbmd0b25wb3N0LmNvbS90ZWNobm9sb2d5LzIwMjQvMDQvMDkvbW9zdC1pbXBvcnRhbnQtYXBwLXlvdXR1YmUvIn0.hHx0Fc4PnGvPN_JJ0hakZ6EE7xwisaHAM2ncHyQAq3o&itid=gfta (Accessed: 11 April 2024).

[19] Standards include app style guidelines, identifying all data collected by the app and identifying if and who the third party-partners are that collect data, reviewing and keeping up to date on Apples changes in privacy rules, identifying if any third-party code was used for the advertising of or selling of personal information and if so what the data is, and conforming to any and all applicable United States laws. Inc., A. (no date) *App Privacy Details - App Store*, *Apple Developer*. Available at: https://developer.apple.com/app-store/app-privacy-details/#data-type (Accessed: 14 March 2024).

and location tools built into the phone (e.g. GPS, Bluetooth etc.).

While Androids do have similar general privacy settings on the user side, they conversely have fewer obstacles placed between apps and user data. Androids do not have any strict enforcement on their app store, causing the potential for a myriad of data collection practices to occur. Androids also allow access to root files which greatly increases risks of user information being accessed regardless of a user's settings.[20]

These user-side controls over privacy and vulnerabilities based on the make of phone coalesce into potential massive variance in accuracy for a database of collected information. The first cause of accuracy variance is that some data points in the database are less accurate representations of a user then other data points.[21] This could similarly result in databases missing information on some users while having full data on others.[22] This results in law enforcement relying on highly variable databases with user data that could be completely inaccurate.

b. App Developers Incentive for Data Collection

While more accurate, complete information is surely preferable, app developers by no means need to have perfect dataset representations of users to turn a profit. In fact, data brokers,[23] a major revenue source particularly for free apps, will often buy user data in fragments and then either form detailed profiles of individuals or update preexisting ones. App developers will also sell ad space within their app, targeted and personalized to each user based on personal information. Selling this ad space can also work with incomplete data; often app developers will partner with an ad network that acts as a middleman between the app company and advertisers. The ad network takes whatever information an app company can furnish them and combines it with their own fragmentary data, applying algorithms and Artificial Intelligence ("AI") to select the best matching and highest paying ad to display. While some app developers may be able to create more precise profiles, this is not always necessary. Between lax civil privacy laws and revenue found in fragmentary user information, app developers have an obvious financial incentive to record and sell information regardless of exactitude. App developers' designs for the scope and content of information amassed in their databases are disparate but wholly unrelated to the objectives of law enforcement as well as any adherence to constitutional protections thereof.

c. App Developers General Methods for Data Collection

The methods of user data collection available to app developers vary based on the make of smartphone, unique aspects of the operating systems, and the specific prebuilt development tools such as Software Development Kits ("SDK"). One of these are SDKs which provide tools to aid in device-specific app creation such as code debuggers, and collections of prewritten code called "libraries" among others. For Androids, app developers use tools such as Google's Android Software Development Kit (Android SDK). Of its many functions, this SDK helps developers to easily access and record data from the various sensors on the phone such as Bluetooth or Wi-Fi

[20] This is not to definitively say that every Android app will do this, rather that there is a general increased risk for users downloading apps from the Android app store.

[21] e.g. an iPhone app that collects user location data could have one user that enabled "share my location only while app is open" but another user might enable "always share my location."

[22] e.g., an app where some users selected "never share information" or disabling certain tracking features, while others allowed full permissions.

[23] A submarket of data brokers exists called the "location data industry," which is worth over $12 billion.

for geolocation.[24] The SDK can also assist in recording data sent between apps such as what and when a web browser is used for.[25] Similar information can be obtained on iPhones as app developers can use Apple's iOS SDK for data collection from the phone's various sensors. Unlike Android, Apple does include a few more features that limit third party apps' ease of access to personal data like Data Vault; however, apps can still gain access to highly private information.[26] In addition to these SDKs, developers can use other SDKs for conveniently adding additional functionalities to their app such as targeted advertising. Google Mobile Ads SDK, for example, helps developers to easily sell ad space within their app and leave the SDK in charge of picking and showing suitable ads which it determines by collecting user data from the app and phone. Many SDKs track and collect information analogous to this, however there is an underbelly. Groups who create SDKs can siphon off fragments of user data whenever an app uses the SDK, and over time they can compile a database filled with data points on various users.[27] Much of this data scraping is done with little warning or understanding by users. Many would assume private or identifying information like this would never be shared without their knowledge and consent, or at the very least, many would not assume this entire structure exists beneath their apps.

2. Google

a. Information Google Collects

Google quietly amasses information from signed-in users as well as anyone accessing a Google service. By using their websites and apps, including but not limited to YouTube, Google Search and Google Maps, copious amounts of fragmentary data regarding an individual's life are collected; at times, without the user's knowledge. When a device connects to a website, information such as language and geolocation is traded; so, for example, YouTube could determine where a user lives, what language(s) they speak, when they watch videos and on what kind of device. This basic example is from just a single website and doesn't look at the more complex tracking and algorithms used by Google that can provide them with basic facts, as well as fodder for extrapolations such as health issues and sexual identity, for example. Google Search engine, whose stored user queries are searched with reverse keyword warrants, records every user's queries, time of query, language and geolocation. When viewing this kind of information individually, it may seem like a single unrelated data point, however when it is combined with the other data points collected from one or more websites, it creates an image of every major aspect of an individual's life - this assemblage of personal information is referred to as mosaic theory. Google can and does track significantly more than simply user interaction within their apps and search engine. Google's Location History provides a real-time timeline of a user's physical

[24] *Request location permissions : sensors and location : android developers* (no date) *Android Developers*. Available at: https://developer.android.com/develop/sensors-and-location/location/permissions#accuracy (Accessed: 10 March 2024).

[25] *Receive simple data from other apps : android developers* (no date) *Android Developers*. Available at: https://developer.android.com/training/sharing/receive (Accessed: 10 March 2024).

[26] *Protecting app access to User Data* (2022) *Apple Support*. Available at: https://support.apple.com/guide/security/protecting-app-access-to-user-data-secc01781f46/web (Accessed: 11 March 2024).

[27] Wang, H. and Guo, Y. (2017) 'Understanding third-party libraries in Mobile App Analysis', *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)* [Preprint]. doi:10.1109/icse-c.2017.161.

movements based on transit of their mobile device. While the accuracy of this data can be highly dependent on where the device is, it can record routes to work, frequented grocery stores and restaurants, and even the duration spent at those places. Barriers to accuracy such as cellular dead space and physical obstructions, while not an impediment to the goal of pairing sellers to buyers, can gravely skew data for a reverse search. A mosaic could be assembled that draws inferences from bad data: a timeline could seem to show where and when someone appeared to have traveled north on a road when, in fact, they were moving west but the signals were subjected to deflection.[28] This particular example is only possible to a point, however, as deflection is a specific, locality-based phenomenon.

b. Why Google Does These Collections

Google collects user information for two main reasons. First, to better target data to users: provide search results relevant to geographically nearby services, recommend videos according to viewing habits, and provide better routes to work or other frequented destinations. Second, this data enables Google to sell massive amounts of ad space targeted specifically at each of their users; sold ad space makes up over eighty percent of Google's total revenue.[29] When collecting user data, Google's primary intentions, like that of app developers, are not to create a list which law enforcement can easily and constitutionally search.

Personal data is a highly coveted commodity to data brokers, advertisers, adtech middlemen, insurance companies, and even the Federal Government. Unacknowledged and unauthorized access to the data of American citizens is only growing easier to obtain by third parties. For example, as modern cars have become more financially accessible and mandatory for the lives of Americans, many models of cars feature onboard computers connected to a network for GPS and map functionality alongside web surfing and streaming capabilities.[30] But these features are deceptively powerful, allowing companies such as Nissan to find ways to gauge not just vehicle owners' commute and frequented stores, but also their religion, sexual identity and relative sexual frequency.[31] Some companies such as Tesla sell auto insurance packages at seemingly low rates compared to market competitors, however, in their contract agreements, Tesla plainly states their use of the sensors on their cars for monitoring drivers safety on the road as to actively make changes to insurance rates accordingly.[32] Unbeknownst to many drivers, other auto companies such as GM have created agreements with data brokers for the collection of driving data.[33] While some companies have stated that they are using the data for apps which help auto

[28] Zhang, G. and Hsu, L. (2021) 'Performance assessment of GNSS diffraction models in urban areas', *NAVIGATION*, 68(2), pp. 369–389. doi:10.1002/navi.417.

[29] Lin, Y. (2023) *How does google make money? [updated Mar 2024]*, *Oberlo*. Available at: https://www.oberlo.com/statistics/how-does-google-make-money (Accessed: 30 April 2024).

[30] Khan, R. (2023) *New ways android is improving your drive*, *Google*. Available at: https://blog.google/products/android/android-auto-new-features-google-io-2023/#:~:text=The%20number%20of%20cars%20with,driver%20needs%3A%20entertainment%20and%20communication (Accessed: 14 November 2023).

[31] **privacy not included: A Buyer's guide for Connected Products* (2023) *Mozilla Foundation*. Available at: https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ (Accessed: 06 January 2024).

[32] *Tesla real-time insurance: Tesla Support* (no date) *Tesla*. Available at: https://www.tesla.com/support/insurance/tesla-real-time-insurance (Accessed: 05 March 2024).

[33] Hill, K. (2024) *Automakers are sharing consumers' driving behavior with insurance companies*, *The New York Times*. Available at: https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html

owners drive safer, the same companies appear to be selling the data to insurance companies; drivers are reporting insurance rates fluctuating in odd patterns that follow changes in their driving style.[34] Similarly, Smartphones have evolved from being somewhat of a novelty just fifteen years ago, to becoming just as essential as cars with over eighty percent of Americans owning Smartphones.[35] With their portability and features, many Americans now call, text, shop, conduct financial business, email and look up information online while on the move. All of those features have also become essential to daily life, along with the hidden mass brokerage of personal data.

This sharing of information is how advertisers are able to specifically target users, inferencing and matching highly private information for curated ads; pregnancy test kits with diaper deals, your favorite brand of salsa and your financial information with grocery store loyalty cards.[36] When accessing a website, these ads are auctioned off via "real time bidding" where the user data is shared and the company with the highest bid sends their ads to the user. An American user's information is shared with advertisers 747 times a day, according to a report by the Irish Council for Civil Liberties.[37] This all happens within 200 milliseconds after loading a page, on desktops and phones alike.[38]

Whether it be an Android or iPhone, Google collects data through devices; businesses sell this data to advertisers and other parties interested in targeting their resources, ergo the breadth and depth of information about the individual is highly valuable. Behind the scenes, Google stores location history data in their "Sensorvault," a database that is often queried by authorities such as the police.[39] Location history data is stored as complex datasets which are far harder to search through than conventional location data that network providers track. When access to conventional data for a given device is sought, the data has been compiled and stored by mobile network operators for their own business purposes.[40] Sensorvault, however, does not compile its data in the same neat manner, requiring data reviewers to scan through and sort it themselves.[41]

Google's uses for location history also extend to the creation, selling and

(Accessed: 14 March 2024).; GM received backlash for this, and as of March 22, 2024, they have announced that they are no longer working with data brokers; see Hill, K. (2024) *General Motors quits sharing driving behavior with data brokers*, *The New York Times*. Available at: https://www.nytimes.com/2024/03/22/technology/gm-onstar-driver-data.html%20or%20https://arstechnica.com/cars/2024/03/gm-stops-sharing-driver-data-with-brokers-amid-backlash/ (Accessed: 21 April 2024).

[34] Hill, *Supra.*

[35] Howarth, J. (2023) *How many people own smartphones? (2024-2029)*, *Exploding Topics*. Available at: https://explodingtopics.com/blog/smartphone-stats (Accessed: 19 February 2024).

[36] Quiggle, J. (2023) *The ways grocery shoppers' personal information is increasingly being shared - thestreet*, *TheStreet*. Available at: https://www.thestreet.com/retail/supermarket-discount-cards-give-companies-personal-data-shoppers-dont-realize (Accessed: 17 February 2024).

[37] *Mass data breach of Europe and US data* (2022) *Irish Council for Civil Liberties*. Available at: https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf (Accessed: 18 February 2024).

[38] Wodinsky, S. (2022) *This is how often online ads are auctioning off your data every day*, *Gizmodo*. Available at: https://gizmodo.com/how-often-do-ads-sell-your-data-every-day-1848931523 (Accessed: 18 February 2024).

[39] Valentino-DeVries, J. (2019) *Tracking phones, Google is a dragnet for the police*, *The New York Times*. Available at: https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html (Accessed: 20 February 2024).

[40] See Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) ("Wireless carriers collect and store CSLI for their own business purposes . . . ."); Google Amicus Brief, supra note 11, at 14 ("To produce a particular user's CSLI, a cellular provider must search its records only for information concerning that particular user's mobile device.").

[41] Lynch, J. (2019) *Google's sensorvault can tell police where you've been*, *Electronic Frontier Foundation*. Available at: https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been (Accessed: 17 April 2024).

marketability of advertisements, a major source of revenue for the company.[42] Via location history, a user's information such as hometown, workplace, route and method for commuting, stores visited and frequented, hobbies or interests, and various other sensitive locations and information can be determined. With this information, Google can suggest new routes for the user, offer nearby restaurant suggestions, advertise a new store or even show promotional materials like coupons.

This information is not collected with law enforcement and Fourth Amendment rights in mind, it is a part of already obfuscated business practices. The practice of government entities accessing and using this information for surveillance of private citizens unsurprisingly leads to false results and further erodes public trust and privacy rights.

c. How Google Collects Its Data

For the interests of this paper, Google collects this user information from two major avenues: phone geolocation information and search engine queries. IP-based geolocation can also be used to collect data as IP addresses are assigned to devices based on location.[43] Meaning that if an IP address is obtained by law enforcement, they can subpoena ISPs for subscriber information. An important distinction here is that a search warrant seeking to obtain an IP address is not particularized, but using the description of an IP address to seek related information is a particularized search warrant, and so this paper will not be discussing IP geolocation any further than this.

d. Location History from Phones

When location information obtained from cell phones has been collected, cell service providers and app developers access and store the location information. They can then construct timelines from this continual recording of location information. Due to this data being a record in the form of a series of connections, coordinates, and timestamps (depending on what was accessible), it is referred to as location data or location history, or "LD/LH". The recording of location history is not limited to cell phones; all that is required for location history tracking is a portable device capable of transmitting location information. Devices with such capabilities include smartwatches, certain fitness bands, vehicles, and more, all with the potential to reveal highly personal information.[44] This location history data is collected and stored by companies such as telephone service providers, Facebook, and Google.[45]

Interestingly in the case of Google's location history data, Google claims to be able to create a confidence interval radius which captures users in a given location with accuracy averaging only around 68%.[46] Unlike cell providers, Google can at times produce more accurate

[42] United States v. Chatrie, 590 F. Supp. 3d 901, 908 n.9 (E.D. Va. 2022) ("Using 10K filings from Google's parent company Alphabet, FBI Agent D'Errico noted that Google's advertising revenue constituted 85.4% and 83.9% of its *entire* revenue in 2018 and 2019, respectively.")

[43] *What is IP geolocation and how does it work?* (no date) *What Is My IP Address*. Available at: https://whatismyipaddress.com/geolocation (Accessed: 17 April 2024).

[44] Technology, T.O. of *et al.* (2022) *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, *Federal Trade Commission*. Available at: https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal (Accessed: 12 February 2024).

[45] *Ibid.*

[46] Macarulla Rodriguez, A. *et al.* (2018) 'Google timeline accuracy assessment and error prediction', *Forensic*

tracking due to location services on certain Android devices alongside Google services such as Google Maps. Relatedly, they offer users the ability to opt in and opt out of location history data tracking, along with access, editing, and deletion on the user end of their respective personal location history.[47] When compared to CSLI and other tracking data, location history tends to have higher accuracy in many cases due to the aforementioned signals and connections such as Wi-Fi, cell networks and even Bluetooth.[48] By using all of these collection methodologies simultaneously, a device's location is more accurately estimated as each input can be cross-checked with the others, and if one input is fairly weak then another can be used in its place. In the case of the Google Maps app, GPS can estimate a device's location up to 20 meters.

Bluetooth, using radio frequency to share data over short distances, can be used to better inform where a device is located based on Bluetooth scanning. This Android feature functions even if Bluetooth has been disabled on the device. Often without notifying the user, Bluetooth scanning on a device will send information to Bluetooth beacons, allowing for fairly accurate geolocation tracking.[49] These Bluetooth beacons are small white electronic devices found in many urban areas such as malls, grocery stores and restaurants. They eavesdrop on network connections for nearby devices, recording when, where and for how long a device was within range.[50]

Wi-Fi can inform the app of the location of the building one is inside, and cell towers, depending on their location, combine to calculate estimating location accuracy in the tens of meters - far more accurately than CSLI or GPS on their own.[51] The way Google is able to use Wi-Fi from buildings for device tracking is by first recording Wi-Fi connections and their respective locations. This is done through their Street View cars which record images and video for Google Earth and Google Maps. Once this information has been collected, Google compiles it into a database.[52] All of this data can be, and is, used to record the user's movements, substantiate habits, connect the pieces together to form a dataset of personal information that can be sold to advertisers. But these datasets are not basal; between the various sources of data for location history, to habits inferred through the use of AI and other personal information, it would be no cursory task to search through a database of them. When collecting location history, Google works with user data and location data simultaneously, making attempts to cleanly separate personal user data from pure location information, as required by law enforcement investigations, very difficult.

However, for Google this location data is invaluable, so it is no wonder that something as simple as users controlling their location history data would be made formidable. Android users' location information is automatically opted in and shared with Google. In the case of iPhone users,

---

Sciences Research, 3(3), pp. 240–255. doi:10.1080/20961790.2018.1509187.

[47] *Manage your location history* (no date) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3118687?hl=en (Accessed: 03 October 2023).

[48] *How google uses location information – privacy & terms* (no date) *Google*. Available at: https://policies.google.com/technologies/location-data?hl=en-US (Accessed: 26 October 2023).

[49] *Google can still use bluetooth to track your Android phone when Bluetooth is turned off* (2018) *Quartz*. Available at: https://qz.com/1169760/phone-data (Accessed: 07 February 2024).

[50] Bluetooth-Beacons can be accurate up to inches; Kwet, M. (2019) *In stores, secret bluetooth surveillance tracks your every move*, *The New York Times*. Available at: https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html (Accessed: 19 February 2024).

[51] See Google Amicus Brief, supra note 11, at 10; see also Carpenter, 138 S. Ct. at 2218 (recognizing that high technological precision increases the likelihood that a search exists); United States v. Beverly, 943 F.3d 225, 230 n.2 (5th Cir. 2019).

[52] *Data collected by Google Cars* (2010) *Google Europe Blog*. Available at: https://europe.googleblog.com/2010/04/data-collected-by-google-cars.html (Accessed: 19 February 2024).

the Google Maps app must be installed, and the user signed in, with permission given to access location services – users can be signed in with the same account on multiple devices and have location history active on each. So long as the iPhone is powered on, location services "allows apps and websites (including Maps, Camera, Weather, and other apps) to use information from cellular, Wi-Fi, Global Positioning System (GPS) networks, and Bluetooth to determine your approximate location."[53] Once Google Maps has this permission, the device's movements are continually recorded, consequently creating the location history of a user. If a user does not want Google to create their location history, the user must decline access to location services by Google Maps or opt out of Location Services. Opting out, especially on Android devices, is confusing and counterintuitive. Even Google software engineers have admitted being perplexed in emails, mentioning how the UI appears user-friendly but in reality, is exceptionally confounding.[54] Location data tracking settings are not confined to one location and come in misleading, often unknown forms. Both Android and iPhone users have their own complex settings that need to be disabled.

For Android users, this means disabling specific features which, depending upon their device settings, include "sensors (such as accelerometer, gyroscope, magnetometer, and barometer), mobile network signals, and Wi-Fi signals…"[55] Even when Bluetooth has been turned off, Google can still use Bluetooth scanning to report location and time data of previous Bluetooth connections and Bluetooth beacons in range.[56] Disabling scanning on Android devices is more obfuscated than those other settings, buried under five layers of menus: Settings > Security & Location > scroll to Privacy > Location > Scanning.[57]

For iPhone users, the features that must be disabled are: Location Services or Precise Location, various location information settings for iOS System Services and Bluetooth scanning.[58] However, when first opening an app, iPhone users are given a chance to indicate their access preferences with dialog such as "always allow access," "allow access only when using app," "allow once," and "never allow access."[59]

Both kinds of devices also require Web and App Activity to be turned off, as otherwise Google is able to continue tracking via workarounds. Web and App Activity broadly captures a large number of other users' location data which is also included in any data accessed by law enforcement leading to overly inclusive results at the expense of the privacy of thousands of

[53] *About privacy and location services in IOS, ipados, and watchos* (no date) *Apple Support*. Available at: https://support.apple.com/en-us/102515 (Accessed: 17 February 2024).

[54] State of Arizona v Google, 2020-cv-6219, exh 224

[55] *How google uses location information, Supra.*

[56] Kwet, *Supra*; *About privacy and location services in IOS, ipados, and watches*, *Supra*; *Manage your Android device's location settings* (no date) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3467281?hl=en%2F (Accessed: 16 February 2024).

[57] Brandom, R. (2018) *Why does my phone make it so hard to turn off bluetooth?*, *The Verge*. Available at: https://www.theverge.com/2018/2/25/17041440/bluetooth-location-tracking-iphone-android-privacy (Accessed: 17 February 2024).

[58] *How to turn off location services and stop your iphone apps from Tracking you* (no date) *PCMAG*. Available at: https://www.pcmag.com/how-to/how-to-turn-off-location-services-on-ios-devices (Accessed: 15 February 2024).; *Control the location information you share on iPhone* (no date) *Apple Support*. Available at: https://support.apple.com/guide/iphone/control-the-location-information-you-share-iph3dd5f9be/ios (Accessed: 08 February 2024).; Bluetooth scanning on iOS is slower and less accurate than Android devices, but is still used by advertisers; *Community - Silicon Labs* (2021) *Silicon Labs Community*. Available at: https://community.silabs.com/s/article/x-reference-background-scanning-for-advertisements-in-ios-apps?language=en_US (Accessed: 18 February 2024).

[59] *About privacy and location services in IOS, ipados, and watches, Supra.*

American citizens.

> If you're signed in to your Google Account and have Web & App Activity turned on, your activity data on Google sites, apps, and services may be saved in your account's Web & App Activity. Some activities may include information about the general area you were in when using the Google service. When you search for something using a general area, your search will use an area of at least 3 sq km or expand until the area represents the locations of at least 1,000 people.[60]

Deleting already-tracked data requires finding multiple Google web pages that are buried within Google Maps Timeline Settings. Users can choose to "turn location history off," however one must first find the correct webpage as there are multiple pages that refer to turning off location history without ever explaining how to do it.[61] Following the steps on Google's support page, users are told: "Turn **Location History** on or off. If you turn Location history off, *confirm and tap **Pause** and then **Okay*** [emphasis added]."[62] With Location History off, "the places you go are no longer stored." However, this is false as some Google apps will still record location data without informing the user.[63]

Similar to their "Sensorvault," personal data collected from Google Search is recorded for revenue purposes, but its scope and nature become an enticingly rich source of intelligence for law enforcement. Americans who utilize the technological innovations of their cars, cell phones and other devices connected to Google products must reasonably assume to have unwittingly handed over voluminous and significant details of their private life. Most Americans would concur their information is highly private and revealing, a pretense that should lead to it not being easily accessed, yet this data remains a coveted commodity to both public and private entities. The reasons for an individual's online searches or location information are capacious - so too are the number of individuals around them who are caught in the net when this information is used by law enforcement with geofence warrants and reverse keyword warrants to identify unique unknown suspects.

e. Information from Google Search Engine

Obtaining user information from search engines and subsequent reverse keyword searches are possible due to the widespread adoption of the internet and the search engines used to navigate its billions of documents and websites. Much like how homes or businesses have physical addresses to send and receive paper mail, every device connected to a computer network has an address. These addresses are dubbed IP ("internet protocol") addresses. IP addresses are used to host websites by acting as an access point and used by the devices to connect to the sites by exchanging packets of information. These packets record the source IP address, such as a

---

[60] *How google uses location information, Supra.*

[61] There are webpage's which reference the ability to turn off location history, yet the steps are hidden within the second link on a subpage accessed via a link on the right hand side of the page; *Manage your location history* (no date) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3118687?hl=en#zippy=%2Cuse-a-web-browser%2Cuse-the-google-maps-app (Accessed: 17 April 2024).; *Manage your location history* (no date) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3118687?hl=en&ref_topic=7189122&sjid=11856657737501244441-NA (Accessed: 17 February 2024).

[62] *Manage your location history* (no date) *Google Account Help*. Available at: https://support.google.com/accounts/answer/3118687?hl=en (Accessed: 17 February 2024).

[63] State of Arizona v Google, *Supra.*

computer, along with a request to access a specific resource of a domain, such as the information to display the homepage of a website. However, this process is bulky so, to make it easier for humans, Domain Names System ("DNS") lookup is used to translate, or "map", human readable domains to IP addresses; much like how a phonebook mapped names to phone numbers. Uniform resource locators ("URLs"), provide a simple way of locating information from human readable domains: first it gives the protocol, then the domain name, and finally the path and query string. For example, the URL "https://www.columbia.edu/content/research" points to the resource "research" which is accessed through the resource path "/content/research" on the domain "columbia.edu."

During the 1990's and early 2000's when the internet was smaller, people used structures like webrings to link and circulate websites. With 1.13 billion websites on the internet currently, the number of URLs has exploded and something more sophisticated than webrings is necessary for traversal. Although search engines starting with Archie had existed since 1990, it would take a few more years before they were robust enough to be useful.[64] Navigating without search engines, or browsers, is like using a phonebook to find an address without a name; if you were to go searching for the address of a business, doing so without the assistance of a browser is time intensive and limited in scope. And in the case of computers, this would be entirely impractical if not impossible, so search engines do the exploring, seeing as much of the web as possible then recording what and where things are found. This way, users only have to provide "keywords" (the list of words that comprise their search) and the search engine can provide URLs that match the keywords.

While there are a large number of search engines globally, focus will be given exclusively to Google Search because it holds the largest search engine market share in America.[65] Generally, search engines operate by first using crawlers to explore webpages, then they index to record the website URL alongside analyzing both the website's code and the rendered website's pages; finally, the search engine uses algorithms to select and sort the webpage links to appear on the search engine results page ("SERP") employing the keywords in a user query.[66]

Crawlers, also known as web crawlers or spiders, are defined as software applications that systematically explore locations on the web by visiting links. These crawlers record information about a given website by recursively following every hyperlink on each page of the site, tracking whether the website is accessible—if error codes are received when attempting to use the website's URL—and recording the HTML and renderings of the website's pages.[67]

The second step, indexing, requires the search engine to review all the information provided by the crawler, then store and sort the URL along with keywords, titles, images, videos and other content found on the page.[68] This provides easy access for the search engine to retrieve its own records of websites.

---

[64] Haan, K. (2024) *Top website statistics for 2024*, *Forbes*. Available at: https://www.forbes.com/advisor/business/software/website-statistics/#:~:text=1.,are%20actively%20maintained%20and%20visited (Accessed: 08 April 2024).; *The history of web search engines: What came before google?* (2020) *WhoIsHostingThis.com*. Available at: https://web.archive.org/web/20210427195319/https://www.whoishostingthis.com/resources/history-search-engines/ (Accessed: 08 April 2024).

[65] *Search engine market share worldwide*, *Supra.*

[66] Harvey, L. (2018) *How search works*, *web.dev*. Available at: https://web.dev/articles/how-search-works (Accessed: 04 April 2024).

[67] Harvey, *Supra.*

[68] Harvey, *Supra.*

In the final step, algorithms are used for compiling a list of websites based on the search query. The search engine takes the user's search terms, breaks them into keywords and applies algorithms to best match the keywords to an indexed URL. Based upon this, the search engine results page is created.[69] In order for these algorithms to produce the most accurate results page, they collect and reference data on the user. By logging a user's universal search history, Google predicts user preferences to help sort results. Geolocation and other location services, search habits, time of day, cookies,[70] and user history on other Google-owned sites such as YouTube, are all used to hyper-refine search optimization at the cost of user privacy.[71] Users cannot edit or delete these logs.

From the 5.35 billion internet users globally, there are approximately 8.5 billion Google search queries each day.[72] These queries can reveal a great deal about the individual or lead to mischaracterization through lack of context due to the short, "intent-based" formulation of most queries. A 2022 research article created a database of the 160 million most popular keywords and broke them into a distribution across four categories by intent: 19.3% transactional, 10.1% navigational, 10.6% commercial and 60% informational, e.g., 'coffee calories,' tend to be more nuanced than most, in that the same topic or search intent can be phrased in a number of different ways to trigger specific results."[73] Out of all searches analyzed, they found 83% were composed of five or fewer words.[74] These statistics can be very helpful for marketing teams optimizing website visibility and understanding specific interests of users, but the data does not allow for easy comprehension regarding why users specifically chose their search terms.

Queries range from medical questions, religious ponderings, physical addresses and views on contentious political issues to name but a few. Users might be trying to diagnose or get help with treatment for symptoms, learn about a new medication they started, or look up a pharmaceutical drug they heard about. When users search something online, their queries are rarely written in full, grammatically correct sentences. Rather, searches tend to be short strings of specifically chosen words that convey basic intent which, under some circumstances, could lead to ambiguous conclusions regarding the user's objective. Take, for instance, "how is blue meth made." To some, this could appear suspicious - perhaps the user is wanting to know how to create meth. Or it could simply be related to how the prop meth was created for the television show *Breaking Bad*. Based on search statistics, users might have chosen this shorter query over something akin to "how is the prop for blue meth from Breaking Bad created"; the two differ in phrasing yet one can still reasonably see a connection. It is believed when TV viewers see something interesting, they tend to search it online out of curiosity.[75] Of these searches, over 60%

---

[69] Harvey, *Supra.*

[70] A cookie is a simple text file which can document, among other things, information identifying a computer's connection to a network.

[71] *What a search engine tracks about me* (no date) *WhatIsMyIP.com®*. Available at: https://www.whatismyip.com/what-search-engines-track-about-me/ (Accessed: 04 April 2024).

[72] Mohsin, M. (2023) *10 google search statistics you need to know in 2023*, *Oberlo*. Available at: https://www.oberlo.com/blog/google-search-statistics (Accessed: 04 April 2024).; *Digital around the world - datareportal – global digital insights* (no date) *DataReportal*. Available at: https://datareportal.com/global-digital-overview (Accessed: 04 April 2024).

[73] Oberstein, M. (2022) *The State of Search 2022 Global Report*. rep. Boston, Massachusetts: Semrush, pp. 22–22.

[74] *Ibid*, pp. 24–24.

[75] *What is the impact of TV on search?: GottaBe!* (2022) *GottaBe! - field and experiential marketing agency*. Available at: https://gottabemarketing.co.uk/digital-marketing/what-is-the-impact-of-tv-on-search%EF%BF%BC/#:~:text=What%20impact%20does%20TV%20have,sticks%20in%20the%20consumer%27s

do not include any kind of branded words.[76]

A query to find a Planned Parenthood center might be for some violent intention, or for a very common rationale like STI treatment. The private address of a house might be searched to stake out a crime, or to get an understanding of the local housing market. To further confuse identifying user rationale, searches can be easily influenced by user geolocation, queries of other users, and typos.

Simply looking at search history to create inferences about the user lacks fundamental context for precisely why and when queries are constructed in a particular manner, since search engines do not need, nor ask for, the logic behind a search. Features such as Google's "People also ask," autocomplete, search bars displaying common searches based on what is in the search field, and typos further facilitate this convolution by creating red herrings not indicative of the user's original intention for a search. "People also ask" is a common feature to appear on search engine result pages; it suggests web pages based on different components of the user query to mixed results.[77] The suggestions might not be similar to the user's search at all, but with one curious or wrong tap will lead to new searches. A search engine's autofill applies predictions concurrently to user input via algorithms, geolocation, search history, and other pieces of information collected for search engine result pages.[78] Users then receive more search engine results for businesses near their geolocation as search suggestions, indicating past and current services they require. While this feature works to provide accurate completion, it can still lead to unintended results or even harmful content (sexually explicit, hate speech, violent depictions, dangerous and harmful activity etc.) especially for queries that are more unique.[79] Connected to results from the autocomplete feature, Google offers previous searches and "common and trending queries" underneath the search bar. The autocomplete feature tries to predict what a user will search as one is typing it.[80]

Google's primary revenue source is selling targeted ad space which is directly tied to user personalization. Through the use of AI and complex algorithms, the contents of a user's previous searches will not only narrow subsequent searches based on similarity, but also tailor specific ads. By having better personalization compared to other search engines, people will find Google to be easier to use, thus increasing foot traffic and total sold ad space.[81] Starting in 2009, Google introduced cookie tracking of anonymous users' location and previous searches for better search results.[82] This addition also helped with personalized ad targeting by linking very specific user information with their browsing history. In recent years, Google has stated they are moving away from personalized searches, yet they have become far less transparent about how their products work. Surprising many, it wasn't until mid-2017 that Google stopped scanning emails for use in

---

%20mind. (Accessed: 14 February 2024).

[76] Raphaelle (2019) *The impact of TV on search*, *NEWS, TECHNOLOGY The impact of TV on search*. Available at: https://blog.realytics.io/en/the-impact-of-tv-on-search (Accessed: 15 February 2024).

[77] *'People also ask' boxes revisited: What are they up to now?* (2023) *STAT Search Analytics*. Available at: https://getstat.com/blog/people-also-ask-revisited (Accessed: 15 February 2024).

[78] Sullivan, D. (2018) *How google autocomplete works in search*, *Google*. Available at: https://blog.google/products/search/how-google-autocomplete-works-search/ (Accessed: 15 February 2024).

[79] *Ibid*.

[80] Sullivan, D. (2020) *How google autocomplete predictions are generated*, *Google*. Available at: https://blog.google/products/search/how-google-autocomplete-predictions-work/ (Accessed: 15 February 2024).

[81] Gennaro-Cuofano (2024) *How much money does Google make from advertising?*, *FourWeekMBA*. Available at: https://fourweekmba.com/how-much-money-does-google-make-from-advertising/ (Accessed: 15 February 2024).

[82] Sullivan, D. (2022) *Google now personalizes everyone's search results*, *Search Engine Land*. Available at: https://searchengineland.com/google-now-personalizes-everyones-search-results-31195 (Accessed: 16 February 2024).

personalization. The harm of this comes not just from the use of personal information, but how little users know and understand what is being done with their information. As The Verge points out, Google's personalization can be troubling to say the least:

> Personalized search results aren't necessarily nefarious on their own. But the ways Google's algorithms function — especially those that are now aided by complex and often unexplainable artificial intelligence software — are and always will be outside the understanding of the common user. By definition, that means most people have no idea how they work, including lawmakers and members of privacy watchdogs and advocacy groups.[83]

Even as awareness of this convention grows for users, Google still is able to maintain a strong chokehold on user data, essentially allowing no user to properly control their own information.

The majority of Americans searching online do so on Google.[84] Users' information is automatically recorded when they are logged into a Google account, watching videos on YouTube or browsing the web through Google Search. In fact, Google stores *all* past searches by users including exact timestamps for each query.[85] Even when not signed into a Google account, searches are still recorded via tracking IP addresses and their associated internet service provider using a unique cookie.[86] If users want to prevent further tracking while signed out, they must either use "incognito mode" which prevents cookies from being used, or stop using Google products altogether. Users who want their search history removed from Google's databases but were not signed into an account have little to no options.

Being that people use Google search for many reasons and the sheer number of queries a day, it is difficult for law enforcement to feasibly narrow their search parameters. Given that Google is not collecting the context for precisely why someone searched something, law enforcement has to make ginormous leaps in logic to determine if the query is at all connected to an investigation. Further, this collection is not restricted to users signed into Google as searching on Google while signed out, or even in private mode; all these could be reasonably used by a user who believes doing so will keep their queries from ready access. As for the general act of searching these sort queries, it could be incredibly misleading for law enforcement as unless an extremely specific, word-for-word query is searched for, many irrelevant queries and personal information can be found.

3. Network Providers

a. The Collected Information

Cell network providers collect geolocation data from devices moving and connecting to various cell sites. When recording these connections, the network providers also track time on the network and device ID. ISPs collect location information such as websites connected to, duration

---

[83] Statt, N. (2018) *Google personalizes search results even when you're logged out, new study claims*, *The Verge*. Available at: https://www.theverge.com/2018/12/4/18124718/google-search-results-personalized-unique-duckduckgo-filter-bubble (Accessed: 16 February 2024).

[84] *Search engine market share worldwide*, *Supra.*

[85] Johnson, L. (2016) *How to see every google search you've ever made*, *How to see EVERY Google search you've ever made*. Available at: https://www.digitalspy.com/tech/a805172/how-to-see-every-google-search-youve-ever-made/ (Accessed: 16 February 2024).

[86] Seymour C.A.R. 21 Pet., Exh. 4 (Nov. 12, 2021 Prelim. Hr'g Tr.), 197:7–10 (Testimony of Special Agent Mark Sonnendecker).

of connections, devices used, and geolocation. To recall when and where a device's connections occurred, providers rely on a device's ability to use network connections, Wi-Fi and GPS. So, when someone moves while keeping a cellphone on their person, the phone effectively visits the same places as the person. On a cursory level, smartphones do this using location-based services: software that reads the device's geolocation – if the user allows it – in real time and sends the information to the software owner's servers for storage and processing.[87] While the accuracy is generally reliable, it can vary for a number of reasons.[88]

Cell site technology enables mobile devices to connect to telecommunication networks – essentially a joined series of satellites, satellite dishes, servers and or towers that carry signals – by emitting radio frequency signals or "pings."[89] These signals are received by the various cell sites that are serviced by mobile network operators (MNOs): private network providers like Verizon and AT&T.[90] Cell towers nearest to a device collect how long and how much data the device uses while connected to the tower. Beginning through these cell towers, the location of the device is also determined by means of triangulation via analytics received from all cell towers within range of the device. A device continually pings nearby towers, connecting to them based on which has the strongest signal strength. This obtained location data is known as Cell Site Location Information, or "CSLI," the records of which are also maintained by the cell network providers.[91] Unless a device has been powered off, this collection is generally unavoidable by the device owner, leading to the assumption that those who wish to use a phone are subject to this collection even if the use of obtained data is against a device owner's wishes, as this data is needed by service providers for billing use of their network.

b. Cell Network Providers Reason for Tracking Information

Major reasons that network providers collect geolocation data are for billing, call tracing, and engineering purposes. By knowing when, where and whose device was using the cell network, the device owner can be charged accordingly. Cell network providers also use data for activation of call tracing; checking and confirming the location of a calls' origin. Network engineering is the other main use as by tracking cell site loads, network providers can determine if and where new cell sites are needed to meet demand.[92]

c. How Network Providers Collect Information

When using CSLI for determining device locations, several factors can work for and

[87] 'location services' (no date) *Pc Mag*. Available at: https://www.pcmag.com/encyclopedia/term/location-services (Accessed: 16 February 2024).

[88] *Ibid*.

[89] Center for Devices and Radiological Health (2022) *Radio Frequency Radiation and cell phones*, *U.S. Food and Drug Administration*. Available at: https://www.fda.gov/radiation-emitting-products/cell-phones/radio-frequency-radiation-and-cell-phones (Accessed: 16 February 2024).

[90] *Understanding Wireless Telephone Coverage* (no date) *Federal Communications Commission*. Available at: https://www.fcc.gov/consumers/guides/understanding-wireless-telephone-coverage-areas (Accessed: 16 February 2024).

[91] Rosenworcel (2022) 'Letter of Inquiry on T-Mobile Data Privacy Practices'. Washington DC: FCC.

[92] *How wireless carriers select site locations* (2023) *Steel In The Air*. Available at: https://www.steelintheair.com/how-wireless-carriers-select-site-locations/ (Accessed: 23 April 2024).

against accuracy, allowing for the possibility of misrepresentative data. Over the years, CSLI has seen increased precision that is quickly approaching GPS accuracy as cell providers have increased coverage in high-traffic areas, reducing the amount of strain on networks that formerly resulted in lowered performance and accuracy. Cell providers have also created more powerful and accurate means for handling coverage.[93] Moreover, when combining CSLI with other geolocation methods such as Wi-Fi, the data collected can produce very detailed timelines of when and where users are located. However, CSLI signals can still be obstructed. Take for instance multipathing, a major cause of inaccuracy, which is when a radio frequency signal is sent to a receiver but instead of the receiver obtaining the single radio signal the receiver gets multiple copies.[94] The result is that the receiver combines the multiple duplicates for an inaccurate reception of the signal.[95] This is due to the radio signal encountering an obstruction that deflects the signal resulting in duplicates.[96] Objects that can cause multipathing distortions are surfaces that are radio frequency-reflective which are mainly "surfaces, such as, furniture, walls, or coated glass" or are metallic in nature.[97] Other common areas and objects are manufacturing areas, distribution centers, metallic racks and shelves, and even office wall dividers, all of which can cause issues like data corruption, signal nulling, increased signal amplitude (known as upfade), and decreased signal amplitude (known as downfade).[98] While buildings, trees, large objects and even shrubs have the potential to block local signals—especially in cities—signal blocking has been less of an issue than it was historically.[99] Formerly, propagations of the signal allowed it to move around objects such as buildings via diffraction, in which a wave expands or widens after it moves through a narrow space or edge, but which would result in the wave "incur(ring) severe loss of power in the process" or "shadowing".[100] Much of this was due to cell towers being spread as far apart as possible to create larger covered sectors, though again, the coverage was not always all encompassing so pockets would be left without service - "dead spots".

Signal corruption has drastically changed, as from 2019 to 2021 alone there were over 69,000 more cell base stations added to coverage areas.[101] Cell base stations can include cell towers but the term "cell base station" is not solely synonymous with cell towers. These newer cell base stations are a compact variety ranging in microcells, picocells and femtocells bringing the national total to over 419,000 base stations.[102] These small cells' coverage areas and powerful broadband

[93] Carpenter v. United States

[94] Rpremach, N. (2021) *Multipath and diversity*, *Cisco*. Available at: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/27147-multipath.html (Accessed: 08 February 2024).

[95] *Ibid*.

[96] *Ibid*.

[97] *Ibid*.

[98] *Ibid*.; *Propagation revisited: Wireless multipath* (2023) *Control Engineering*. Available at: https://www.controleng.com/articles/propagation-revisited-wireless-multipath/ (Accessed: 06 January 2024).

[99] Young, W.F. *et al.* (2010) 'Radio-wave propagation into large building structures—part 1: CW signal attenuation and variability', *IEEE Transactions on Antennas and Propagation*, 58(4), pp. 1279–1289. doi:10.1109/tap.2010.2041142.

[100] *Ibid*.; *Diffraction* (2024) *Encyclopædia Britannica*. Available at: https://www.britannica.com/science/diffraction (Accessed: 08 February 2024).; Andrews, J., Ghosh, A. and Muhamed, R. (2007) in *Fundamentals of WiMax: Understanding Broadcasting Wireless Networking*. Englewood Cliffs, NJ: Prentice-Hill, pp. 24–24.

[101] (2022) *CTIA*. Available at: https://www.ctia.org/news/2022-annual-survey-highlights (Accessed: 09 April 2024).

[102] 'House Committee on the Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services', *Supra.*

powered by millimeter wave technology have been massively adopted in dense urban environments.[103] As computer scientist Matt Blazes explains, these cells are "designed to serve very small areas, such as particular floors of buildings or even individual homes and offices."[104] And as with large cell base stations, these small stations transmit device locations, rendering devices in urban areas trackable with great precision down to individual buildings and even floors.[105] Diversity, the use of two antennas for one radio frequency signal, also helps address multipath issues. The two antennas are spaced away from both each other and the radio frequency transmitter as this lessens the possibility of multipath propagation.[106] One of the two antennas will potentially receive a more accurate non-radio frequency null signal.[107] Though in rural areas, accuracy can still be poor, at times resulting in the ability to pinpoint a device in only miles. Again, when using CSLI alone to determine a device's location a range of potential issues can exist, so context and great amounts of specificity should be given to the data before it can come closer to being a reliable means to determine the location of its associated user.

When combined with Wi-Fi or GPS, CSLI's potential shortcomings can be lessened. While in theory this combination would result in greater accuracy, such a state cannot be guaranteed. If location services are allowed to combine CSLI and Wi-Fi, the device will be more accurate as data from Wi-Fi collection will counteract the cell signal obstructions that often occur indoors. Combining just CSLI and Wi-Fi produces accurate location tracking only to a degree, but when paired with technologies such as GPS, it results in far more efficient and accurate location positioning.[108] GPS used on its own has the capability for extremely accurate location tracking due to differential GPS. Differential GPS involves a fixed reference point repeatedly transmitted to multiple points via satellite, creating a differential correction, improving the accuracy of the fixed point over time.[109] When combining GPS with Wi-Fi, location can be determined with high precision so long as the device is in an area with dense Wi-Fi signals. Any blockages that might occur in the GPS accuracy like weather or building density can be counteracted by the Wi-Fi. As with all other iterations and combinations for location services, this too requires that all the desired technologies' requisite conditions be met. If all conditions were perfectly met, databases could be filled with extremely precise tracking data spanning a device's location throughout the day, a very chilling result.

II. Legal Background

Reverse search warrants are increasingly being applied by law enforcement to track down criminal suspects. Unlike more "traditional" search warrants, reverse search warrants are not

[103] *What is small cell technology?* (2022) *Verizon*. Available at: https://www.verizon.com/about/our-company/5g/what-small-cell-technology (Accessed: 04 February 2024).

[104] 'House Committee on the Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services' (2010), pp. 7-9.

[105] *Precision planning for 5G era networks with small cells* (2019) *5g Americas & Small Cell Forum Whitepaper*. Available at: https://www.5gamericas.org/wp-content/uploads/2019/10/SCF-Precision-Planning-WP-FINAL-1.pdf (Accessed: 18 February 2024).

[106] Rpremach, *Supra.*

[107] When two signals cancel each other out resulting in no signal being received; Rpremach, *Supra.*

[108] Paek, J. *et al.* (2011) 'Energy-efficient positioning for smartphones using cell-ID sequence matching', *Proceedings of the 9th international conference on Mobile systems, applications, and services* [Preprint]. doi:10.1145/1999995.2000024.

[109] Srivastava, G.S. (2014) *An introduction to geoinformatics*. New Delhi: McGraw Hill Education (India), pp. 227-227.

written to sweep for evidence; rather, they seek individuals who otherwise would have remained unidentified in the investigation without the search's resulting data. Instead of specifying an individual connected with a crime, reverse warrants electronically search everyone within a specified window of time by either an online queried keyword or geolocation. This methodology inevitably searches the information of individuals wholly unconnected with the criminal investigation. As such, these searches have presented novel questions to the Fourth Amendment, with some privacy experts arguing that law enforcement's rationale for employing these wide net casts borders on mere hunches.[110] Moreover, privacy experts are concerned whether reverse searches adequately adhere to modern legal readings of particularity and probable cause as said searches must search everyone in a database on the premise that the perpetrator could otherwise elude apprehension for lack of evidence.

Geofence warrants assume that the unidentified suspect carried a powered-on smartphone with Google Maps or other similar location service-based app(s) to justify a search of everyone within the determined timeframe and area. Keyword warrants rely on assumptions about what the unidentified suspect queried online and further assume that the query is both reason for suspicion and unique enough to not unduly search innocent persons. So, the questions become if this reasoning is indeed analogous to a hunch, and if said reasoning is sufficient to support searching everyone in a location, or everyone who queried a phrase, in order to pinpoint an unidentified suspect. Further, should this be indicative of a lack of individualized probable cause, or could reverse warrants still be argued as trawling through information to find something that matches broad, vague parameters and is evidence of lacking probable cause to search that location. Additionally, do they fail to narrow broad search parameters to sufficiently meet particularity, as extensive location or keyword criteria could potentially lead to revealing unrelated crimes. There is also the issue that when reverse warrants find a match, it could trigger a Fourth Amendment search on the individual.

A. Defining the Fourth Amendment Requirements

The Fourth Amendment under the Constitution originated in reaction to the unfair prejudice experienced in the American colonies and political dissonance in England. Sentiments were growing that while English Law had one hundred years previously celebrated the maxim “every man’s house is his castle,” it was not so for the common colony folk.[111] They were often victims of “writs of assistance” executed by the British who were driven by animosity and other biases to intrude on private property, rummaging around and seizing personal belongings as evidence for wrongdoing. In England, the 1764 case Entick v. Carrington saw the precipice of this inequality when the writer John Entick, who was accused of producing seditious works in his newspaper, was subjected to a forcible, destructive, top-to-bottom search of his property.[112]

Searches very similar to this for smuggling were occurring in the colonies. Supported again by “writs of assistance,” termed general search warrants, the Crown intruded upon many homes, vaguely searching then seizing any “men and goods prohibited and uncustomed.”[113] These

[110] People v. Seymour, 526 P.3d 954 (Colo. 2023)

[111] 5 Coke’s Repts. 91a, 77 Eng. Rep. 194 (K.B. 1604)

[112] Entick v. Carrington [1765] EWHC K.B. J98

[113] 'Charles II, 1662: An Act for preventing Frauds and regulating Abuses in His Majesties Customes.', in Statutes of the Realm: Volume 5, 1625-80, (s.l, 1819) pp. 393-400. British History Online https://www.british-history.ac.uk/statutes-realm/vol5/pp393-400 [accessed 23 April 2024]

warrants remained valid for the lifetime of the King under which they were written so upon the death of George II there was immediate resistance against the creation of any more of these warrants. Thus, when the Fourth Amendment was later written for the protection of United States' citizens, memories of abusive general search warrants drove new safeguards for private property and the papers and effects found therein. Until relatively recently, searches defined under the Fourth Amendment only concerned tangible space; i.e., the trespass of a physical, private, constitutionally protected space to search for information by employee(s) or agent(s) of the government.[114] It is understood by doctrine that in these physical searches, the information desired would not be in public view, as were it in public view, the owner could not expect privacy from the eyes of the public. This public view, developed under reasonable expectations of privacy, suggests that officers require a warrant for search and seizure if the observation or access to something requires the officers to be in a location or situation that violates the Fourth Amendment.[115] However, these limitations must now be understood with the rise in use of digital devices and subsequent reverse warrants. Modern phones and computers can hold and record far more complex, personal information than a house ever could. The contents of a phone or computer are only observable if powered on and unlocked or the information is somehow extracted through electronic means; even so, much of the information relevant to reverse warrants, such as location tracking, is retained by third-parties - companies such as Google. This has brought forth a new question of whether individuals should have an expectation of privacy under the Fourth Amendment when the information is highly revealing and in digital space, yet is stored and accessed by companies; likewise, how evolving technology impacts both privacy and applications of search warrants.

1. Kyllo v. United States (Decided 2001)

Kyllo v. United States helped redefine what type of spaces are protected under the Fourth Amendment within specific sectors of modern technology. Thermal imaging was used by United States Department of the Interior agent William Elliott from a public street to scan for specific heat waves in petitioner Danny Kyllo's home in order to confirm suspect activity. The issue regarded whether the employment of a device not in general public use in order to remotely search a premises constituted a Fourth Amendment type search. Elliott had reason to suspect the owner of the home, Kyllo, of illegally growing marijuana inside his home. Specific halide lights are required to grow marijuana indoors which can be detected by scanners. Using a thermal imager capable of detecting infrared radiation which is invisible to the human eye, Elliott performed a scan of the house while sitting in the passenger seat of his vehicle across the street from the front of the house and from a street facing the back of the house. The scan revealed a greater amount of heat coming from the roof of the garage and a side wall compared to the rest of the house and of nearby houses. Using this imaging, along with informants and utility bills, a search warrant was obtained and executed on the petitioner's home revealing over one hundred marijuana plants and confirmed the presence of halide lights, implicating the petitioner in an illegal grow operation.

The case was brought to the Court of Appeals for the Ninth Circuit on grounds of the intrusiveness of thermal imaging. The District Court found the thermal imaging device used to be "a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house;" it "did not show any people or activity within the

[114] United States v. Jones
[115] Collins v. Virginia, 138 S. Ct. 1663 (2018)

walls of the structure;" "[t]he device used cannot penetrate walls or windows to reveal conversations or human activities;" and "[n]o intimate details of the home were observed."[116] The District Court held the validity of agent Elliott's warrant and ultimately the Court of Appeals held that Kyllo had no expectation of privacy as he had not attempted to block the halide lights' warmth from detection. Even had he done so, he could still not claim an expectation of privacy as the scan "did not expose any intimate details of Kyllo's life," only "amorphous 'hot spots' on the roof and exterior wall;" the Supreme Court then granted certiorari.

After hearing the case, the Supreme Court found that this scan did violate the Fourth Amendment as it is not reasonable for a person to expect that such a device would be used on their house, nor should they be expected to secure their private affairs in such a way that they would be hidden from thermal imaging devices. In essence, this affects law enforcement such that they cannot wield technology such as the thermal camera which is "sense-enhancing" in order to obtain information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" while skirting constitutional scrutiny.[117] Moreover, in the opinion of the court, Justice Scalia made clear that rising technology beyond what is seen in this case, does impact the constitution: "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Search warrants utilizing advancing technology impact how the Fourth Amendments' protection for citizens as in cases such as this, the technology can be used for blind surveillance.

> To begin with, there is no necessary connection between the sophistication of the surveillance equipment and the "intimacy" of the details that it observes–which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful… even when (if ever) that jurisprudence were fully developed, no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up "intimate" details–and thus would be unable to know in advance whether it is constitutional.[118]

This use of advanced technology allows law enforcement to view intimate details blindly - they would learn of details not connected to their investigation as their warrant allows them to search too broadly; if it did not, what other conclusion would it lead to if they could so unpredictably see intimate details. The issue is that rising technology can allow for unparalleled powers of search which could not be recreated without physical intrusion into a space. Further, such technology in a search warrant cannot be reliably proven to narrow where to search and what is to be searched for - they are not just viewing details of a home from the street with the naked eye. The Fourth Amendment "requires clear specification of those methods of surveillance that require a warrant," yet these technologies cannot demonstrate such clear specification.[119]

The so-called "two-pronged test" from Katz v. United States is the description of reasonable expectation of privacy from a Fourth Amendment search given by Justice Harlan, "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'." The Kyllo court in-part, built their decision off of this by extending understanding of Fourth Amendment searches to conclude the definition of a "search" to be either: (1) trespass of a physical, private constitutionally protected space to search for information by employee(s) or agent(s) of the government, or (2)

[116] Kyllo v. United States, 533 U.S. 27, Supp. App. to Pet. for Cert. 39—40.
[117] Kyllo v. United States, 533 U.S. 27 at 34 (quoting *Silverman*, 365 U.S., at 512) (2001)
[118] Kyllo v. United States, 533 U.S. 27
[119] *Ibid.*

when an individual's *subjective* expectation of privacy has been violated by employee(s) or agent(s) of the government in such a way that society is willing recognize as an expectation of privacy.[120] Stemming from the initial Katz test, the Court would also later affirm that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," which created the third party doctrine.[121]

2. United States v. Jones (Decided 2012)

United States v. Jones assessed rising technologies and their impacts on Fourth Amendment searches stemming from physical trespass. While this case is not about searching technology as an intangible space under the Fourth Amendment, it does help define reasonable durations of tracking and concerns of third-party doctrine affecting information stored using technology. In 2004, respondent Antoine Jones, whose business resided in the District of Columbia, became a suspect of trafficking narcotics by FBI and Metropolitan Police Department task force. Based on surveillance information investigators obtained on Jones, a warrant was applied for authorizing the installation and use of an electronic tracking device on Jones' wife's car. Investigators installed a GPS tracking device onto the vehicle which allowed them to track the vehicle's GPS movements over the course of 28 days, with an accuracy of approximately 50 to 100 feet which was recorded every ten seconds.

With this information, the government charged Jones with a multi-count indictment for conspiracy to distribute and possess with intent to distribute cocaine.[122] Prior to trial, Jones motioned the District Court to suppress the GPS data, however the court only granted the motion in part.[123] The court held that aside from the data collected when the vehicle was parked in a garage next to Jones' residence, the tracking was admissible on grounds that, "'a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'"

At trial, Jones was ultimately found guilty and charged with conspiracy. Jones appealed to The United States Court of Appeals for the District of Columbia Circuit which reversed the conviction due to the admission of evidence that was obtained through warrantless use of GPS.[124] By 2011, the Supreme Court granted certiorari on the case, determining the use of a GPS tracking device constituted a search under the Fourth Amendment. With Justice Scalia delivering the opinion of the court, it was found that because the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," then the Government's intrusion on an "effect," the vehicle, was for obtaining information, and thus the intrusion was a search.

This case helps begin discussions that define citizens' expectation of privacy from GPS tracking with it becoming a search under definition of the Fourth Amendment. In Justice Sotomayor's concurrence, she advances the ideology that voluntarily handing information over to a third party does not automatically bar Fourth Amendment reach. In effect, her concurrence motions the Fourth Amendment's reasonable expectation of privacy test to remain open towards information which might have been handed over voluntarily when the information is complex,

[120] *Ibid.*
[121] Smith v. Maryland, 442 U.S. 735 (1979)
[122] See 21 U.S.C. §§841 and 846
[123] United States v. Jones, 565 U.S. 400 (2012), 451 F. Supp. 2d 71, 88 (2006)
[124] United States v. Jones, 565 U.S. 400 (2012), 615 F. 3d 544 (2010)

such is the case with technology, and whose release to a third party is not understood by the individual. Having little to no understanding of what and how much information is being "voluntarily" handed over could be an avenue where one might project a reasonable expectation of privacy as the meaning of "voluntarily" in this context would be counter to the definition established. This sentiment, as expressed by Justice Sotomayor in her concurrence, laid further groundwork for understanding Fourth Amendment protections and expectations beyond the scope of the technology seen in this case: "[p]eople 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 . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."

3. Carpenter v. United States (Decided 2018)

The new concept for subjective expectations of privacy formed in Kyllo was expanded upon in Carpenter v. United States. Beginning in late 2010, there were a number of robberies of Radio Shack and T-Mobile stores in Detroit, Michigan, eventually leading to the Federal Bureau of Investigation opening an official investigation into the matter in 2011. After investigators arrested four suspects, one of the arrested admitted that all four had been responsible for robberies in Michigan and Ohio. They also furnished investigators with the names of fifteen accomplices along with some of their phone numbers. Under provisions in the Stored Communications Act, investigators are allowed to compel the disclosure of certain records from telecommunication companies so long as the result of said disclosure "offers specific and articulable facts showing that there are reasonable grounds to believe" that records sought "are relevant and material to an ongoing criminal investigation."[125] Investigators applied for Court Orders to obtain cell record location data on a few of the suspects whose numbers were provided; of these, one was petitioner Timothy Carpenter. Under two orders from Federal Magistrate Judges, Carpenter's mobile carriers were then asked to release records of "'cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls' during the four-month period when the string of robberies occurred."[126] The investigators received two records which spanned 127 days and seven days respectively, with a combined 12,898 location points of Carpenter's movements.

During pre-trial procedures, Carpenter moved to suppress the cell-site data on grounds that the Government's seizure of the records violated his Fourth Amendment rights because the Government obtained the records without a warrant supported by probable cause. However, the District Court denied the motion.[127]

After being convicted, Carpenter appealed to the Court of Appeals for the Sixth Circuit which affirmed the previous decision.[128] The court held that due to Carpenter willingly sharing information with his mobile carrier, he lacked any reasonable expectation of privacy. The reasoning behind this was specifically that a cell phone user voluntarily transmits information to

[125] Note that under this the phrase "reasonable grounds" is being used which would mean a standard short of probable cause, 18 U.S.C. §2703(d)

[126] Carpenter v. United States, 138 S. Ct. 2206 (2018), App. to Pet. for Cert. 60a, 72a

[127] Carpenter v. United States, 138 S. Ct. 2206 (2018), App. to Pet. for Cert. 38a–39a

[128] Carpenter v. United States, 138 S. Ct. 2206 (2018), 819 F. 3d 880 (2016)

their cell carrier "as means of establishing communication,"[129] and so their information in the form of cell provider business records would not receive Fourth Amendment protections - third-party doctrine is applied.

Then in 2017, The Supreme Court granted certiorari. With Chief Justice Roberts delivering the decision of the court, it was found that the Government's seizure of Carpenter's cell-site records constituted a Fourth Amendment search. The Court determined that location information held by a third party did not fall into the then-held understandings of personal expectations of privacy of physical location and movements, nor limited expectations of privacy from willingly handing personal information over to third-parties. For the former, the court found the precision that is possible with CSLI to be highly detailed yet CSLI itself to be unique enough such that CSLI was analogous to GPS qualities seen in Jones v. United States but should not have third-party principles extended.

The court reasoned that the case was reliant upon how third-party doctrine was read. They stated that the discussion of third-party doctrine ought not to be solely understood as a reduction of expectation of privacy triggered by an individual willingly handing over information. Instead, it should additionally address "the nature of the particular documents sought" and the subsequent limitations projected onto "[a] legitimate 'expectation of privacy' concerning their contents." The court also concluded that the third-party doctrine's rationale of voluntary exposure needn't apply to CSLI given that one does not share location information such that the act of "sharing" is ostensible to the understanding and used definition of "share" in this context. Inversely, cell phones and cell services are insistently irrevocable to the operations and participation of members in our modern society; secondly, cell service providers recording cell logs are a direct byproduct of the cellphone's function, requiring no action on part of its user beyond turning the phone on.

d. Sub Analysis

The advent of digital expectations of privacy from Kyllo and expanded in Carpenter affirmed that there exists some intangible space under which the timeline and accuracy of evidence via CSLI is equivalent to searching through paper and effects. Carpenter found that individuals do in fact have a reasonable expectation of privacy as CSLI, being but one of many methods for tracking, can reveal the confidentialities of one's life despite the data being collected and stored by a private business wholly unaffiliated with law enforcement. The Supreme Court's opinion reasoned that location history spanning 127 days was an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" Further, the Supreme Court made clear that when analyzing these technologies in light of expectations of privacy, thought must be given not just to the technology used in the case, but also "more sophisticated systems that are already in use or in development." From this, it would be hard not to conclude that technology which provides intimate views into the affairs of an individual should already be approached with great trepidation by law enforcement. Believing otherwise invites opportunity for citizens to be "at the mercy of advancing technology"[130] through its misunderstanding and poor handling within applied warrants.

There is also the two-step test first suggested in Katz v. United States (1967) for understanding expectations of privacy: "1 the individual has exhibited an actual (subjective) expectation of privacy 2 the expectation of privacy is one that society is prepared to recognize as

[129] Smith v. Maryland, *Supra*, at 741 (1979)
[130] Kyllo, *Supra*.

reasonable, 'official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.'"

2. Insufficient to the Particularity Requirement

In order to avoid the dreaded "general search warrant" that broadly sweeps for criminal suspicions or misdoings that "the Framers intended to prohibit," search warrants under the Fourth Amendment must be particularized such that a warrant will "carefully tailor[] [the search] to its justifications."[131] Specifically, the Fourth Amendment provides as protection that a warrant must "particularly describe[] the place to be searched and the persons or things to be seized." This particularity ensures that law enforcement's warrants are limited in their "authorization to search to the specific areas and things *for which there is probable cause to search*."[132] Further, such a limitation ensures "that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another… [a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant."[133]

For technology and reverse warrants, three major issues related to particularity must be contended with: rising technologies can automate or otherwise greatly impact searches in a way which makes them easier to execute compared to a pure physically conducted search; second, reverse warrants seizing unknown information are based off of an inextricably linked *place to be searched*, causing a conflation of the two-pronged requirements of particularity; and finally, the use of time-frames to address concerns of narrowness when the information being searched is massive - databases.

Rising technologies that can be used by law enforcement as "sense-enhancing" enable the collection of information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" and in such a manner that is divergent from the traditional, physical-based intrusions. Crude or otherwise, such technology impacts how the Fourth Amendment defines the idea of human senses and how they can be used. As was the case with Kyllo, viewing a space with the naked eye was distinctive from using thermal imaging as the Fourth Amendment only addresses intimate space and law enforcement's perception with the naked eye. The technology allows for a new depth and ease of access to "intimate" information. As such, because the warrant detects information that an officer could not know otherwise, then it would be impossible to prove particularly such that the search would minimize its intrusiveness in a space that has been proven to be protected from physical intrusion "by even a fraction of an inch." In essence, it is the technology itself that causes the search to be too broad for Fourth Amendment muster. Kyllo also made it clear that the court believes in understanding the long-term effects modern technology could have, "[t]he Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure *when it was adopted*, and in a manner *which will conserve* public interests as well as the interests and rights of individual citizens."[134]

In order to both tailor a search to its justifications and prevent exploratory rummaging, it would follow that a sufficiently particularized warrant must reduce all intrusiveness where it can and examine the least amount of unrelated information. In Riley v. California, the Supreme Court

[131] People v. Seymour, *Supra* (quoting Garrison, 480 U.S. at 84)
[132] Garrison, *Supra*, at 84 (emphasis added)
[133] Marron v. United States, 275 U.S. at 12
[134] Carroll v. United States, 267 U.S. 132, 149 (1925) (emphasis added)

discussed the privacy issues involved with searching cellphones, and why particularly describing the place to be searched of said technology is difficult. While Riley concerns cell phones, the Court's opinion can nonetheless be extended to "minicomputers that also happen to have the capacity to be used as a telephone" as "[t]he term 'cell phone' is itself misleading shorthand."

> …[A] cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record… today[,] many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives… A[] possible rule is to restrict the scope of a cell phone search to information relevant to the crime, the arrestee's identity, or officer safety. That proposal would [] impose few meaningful constraints on officers. Finally, California suggests an analogue rule, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. "If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number." But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form.

Reverse warrants fail to specify particularity due to falsely conflating *what to search for* with *where to search*. Given that the purpose of a reverse warrant is to aid law enforcement when they do not know the information of who they are looking for, then they aim to seize individuals' information via it being linked to information known from the investigation - a search query that shares a connection, or the geolocation of a place of interest. To narrow the search, they "particularize" it by either geolocation or keyword, then seize the user information linked to the geolocation or search query. However, in doing this, no fewer users will be searched than would be with a general warrant as the description of what to seize matches that of where they intend to search, effectively they are seizing specific information in the location they are searching for it.

Looking for something specific does not give law enforcement leeway to search every vague place where the information could technically reside. Doing so requires law enforcement to apply their own discretion when executing the warrant. Furthermore, geolocation and search terms are hardly unique enough to reasonably ensure that they would reveal the relevant crime. True, a search term, say the address in *Seymour v. Colorado*, could be the location related to the investigation, but the address could also be the location of a hair salon, gay bar, Planned Parenthood, and so on. If an address is held as sufficiently narrow, so too could search terms like "AR-15" or "abortion care," either of which could be linked to a crime depending on the location. This bar for "narrowness" seen in addresses would easily catch far too many people who would be unrelated to the crime. Here also exists the issue that using the technology involved is what enables the search to be too broad, as the ease and volume of information being searched is incomparable to that of a physical search.

In an attempt to address the concern of the narrowness of reverse searches, timeframes are stipulated in the warrant. The time ranges from hours to weeks, and while limiting a search through these can shrink the number of individuals searched, its sole use has no impactful effect on the intrusiveness of a search - and in the case of search queries where millions are made each day, the number of searched individuals would still be voluminous. Time frames yielding fewer results do

not make up for reverse warrants inability to determine the number of results prior to executing the search. As was established in Kyllo, not knowing what will be revealed and who will be searched only creates more constitutional concern as such information is protected from view.

3. Lacking Probable Cause

Given that particularity is the narrowing of a search to areas and things of which there is probable cause to search, it would follow that probable cause should be addressed. In order to protect the individual from baseless suspicions and searches, probable cause acts as a co-deterrent with particularity. While the Supreme Court has made it clear that "probable cause is a fluid concept… not readily, or even usefully, reduced to a neat set of legal rules," they have provided a base requirement.[135] Probable cause is seen as setting a higher bar than reasonable articulable suspicion, relying on an officer's knowledge that is "not based wholly or largely on surmise or hearsay; the facts derived from his personal observation were sufficient in themselves, without the hearsay concerning general reputation, to sustain his conclusion."[136] Further, "[a]lthough a mere 'hunch' does not create reasonable suspicion, the level of suspicion the standard requires is considerably less than proof of wrongdoing by a preponderance of the evidence, and obviously less than is necessary for probable cause."[137] Yet technologies used in reverse warrants seem to be unable to narrow their search, signifying that there is a lack of probable cause as law enforcement would be searching without specific suspicion or ability to demonstrate suspicion toward a particular individual.

The result is individuals being searched under the assumption that linking a detail of the investigation to an individual's personal information will pass muster. Holding the belief that some information among a collection of millions could link an unknown perpetrator to an investigation and thus establish probable cause could prove problematic. With reverse warrants, law enforcement would have no reason to suspect any piece of data or information over another in the broad collection. They would be searching massive amounts of data, most of which would be based on surmised information gained based on the results of the search.

Analysis

* * *

Through understanding the Fourth Amendment's protections of intimate space in relation to technology, one can extend the view of protections to new tracking technologies analogous but more powerful to the CSLI seen in Carpenter. We can use CSLI as a baseline to define tracking technology as being capable of recording information in a fashion that is "detailed, encyclopedic, and effortlessly compiled," with CSLI specifically being cited as "giv[ing] the Government near perfect surveillance and allow[ing] it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers."[138] The concept of sense-enhancing technologies implicates the tech used in reverse warrants on spaces containing intimate information as law enforcement's ability to see and remember a person's whereabouts is deeply

[135] Illinois v. Gates, 462 U.S. 213 (1983)
[136] Brinegar v. United States, (1949)
[137] Kansas v. Glover, 140 S. Ct. 1183, 1187 (2020)
[138] Carpenter v. United States, 819 F. 3d 880

enhanced. Even the individual pieces can be weaved together to reveal intimate information or space. This results in many cases of reverse warrants barring law enforcement from ever knowing the degree to which mass numbers of individuals' intimate space will be captured by the search. The application of reverse warrants makes narrowness extremely difficult to achieve, if not at times impossible.

The foremost cause of reverse warrants lacking particularly is rooted in the type of personal information held by the companies being searched, and law enforcement's search methodology given the totality of circumstances. Analysis will be focused on causes of reverse warrants on app developers and Google being unconstitutional, then general models will be presented for how reverse warrants could be applied constitutionally.

A. Constitutional Challenges

When applying reverse warrants to app developers, there could be potential for many users' intimate spaces being collectively and broadly searched. Apps can record any combination of information from movement, the amount of time spent with the app open, activity on other apps, access to contacts and more. Even though a reverse warrant targets just the information connected to the investigation, it can easily include many who are not connected to the investigation due to warrants not particularly searching areas for which there is evidence that the information is reasonably likely to be located. Given the wide range in tracking capabilities an app can have along with inexactitude caused by inaccurate information or even app permissions, the data could contain an array of information that is unrelated to the search and, more pressing, individuals who are unrelated. This could cause false positives, a mosaic of an individual's life, and generally unpredictable search results. Since law enforcement would be using sense-enhancing technology, prior knowledge or control of these searched spaces would be impossible. Unless the set of people being searched was small such that "the warrant [] searched only those places and for those objects that it was reasonable to believe were covered by the warrant," then law enforcement would be searching many people who were not covered.[139] Given this unpredictability in light of information being searched in an invasive way, the results of these searches should not be permissible as the proverbial fruit of the warrant would not match their descriptions as "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false."[140]

Applying search warrants to Google, either geofence or keyword, runs into similar issues of broadness and intimacy. Google collects specific information on their users over a long span, even if the user is not signed in to a Google account. This allows their collected data to contain intimate information that distinctly lacks the users intent for searching something or going somewhere. Google can only surmise intent based off of an algorithm's assessment of a user's intimate habits and information. For geofence, this means that when law enforcement applies their reverse warrant, the sense-enhancing technology coalesces into knowledge of everyone who might have been in a location, with any mismatches needing to be eliminated by officers after the fact. Geolocation can reveal that an individual was at a church, or doctor's office, or home, yet the reverse warrant will treat all these locations the same, even though the home has the strongest guaranteed constitutional protections. Yet, geofence warrants will often include search spaces that would likely contain many individuals with no connection to the suspect as the area is not directly

[139] United States v. Leon, 468 U.S. 897 (1984)
[140] *Ibid*. at 899

or sufficiently related to the crime.[141] Keyword searches' broadness lowers the bar of narrowness such that nonspecific searches would pass muster whose results clearly lack any meaningful or useful connection to a specific investigation. If a users' query contains something illegal or contentious within the state they were in at the time, it would be enough to cast suspicion on them despite them having no clear connection; in effect, treating everyone in a dataset as a suspect.[142]

B. Writing Constitutional Reverse Warrants

Geofence warrants might be able to pass constitutional muster of particularity in situations where the timeframe and location could be proven to contain individuals who had a reasonable chance of being connected to the investigation prior to the search. An instance of this would require the geofence to be limited to a space which is small enough to be reasonably likely to contain the suspect and few others, and whose size is based on the totality of circumstances and available technologies.[143] These two hypothetical examples will be explored: a crime occurred in a remote gas station convenience store around 1:00 to 2:00 a.m., a crime occurred in a mall's outlet store around noon.

Given the gas station problem, the warrant needs to particularly show *where* the search is happening and *what* is being searched for without getting the place to be searched wrong, including space where there is no evidence that the information will reside there, omitting known information in the description, not showing that it is now probable that the information was in the location and will be revealed by the applied warrant, or in a way using broad sweeping language.[144] As such, where the geolocation of search might be drawn could be the gas station store between 1:00 and 2:00 a.m., and perhaps including the gas pumps and parking lot if there is a reasonable chance that the suspect would have needed to navigate through this space in order to get to the gas station.[145] Since law enforcement would know the timeframe, then it is only appropriate to confine the search to that known time and to the space where the suspect would have had to have passed through but wouldn't contain so many other individuals as to mislead the result. Specifying *what* could mean anyone's information identified through their phone information who was present in that location at that time.

For the mall problem, the warrant must address as much of the issue as possible that such a space could contain far more people who would have been in close proximity to the crime but are totally unattached to the crime. If present, accurate technology like Bluetooth beacons can drastically narrow the search area with high accuracy, and in turn, reduce the number of people being searched. So, while there are more people, the search could be restricted to just connections to the beacon between say 11:30 a.m. to 12:30 p.m. Even so, this could still run the risk of being unparticularized if the beacon's range is larger than the space where the suspect would reasonably have been.

Reverse keyword warrants appear to be far harder for which to construct a constitutionally

---

[141] Such as including an apartment building when the crime scene was at a bank; United States v. Chatrie, 590 F. Supp. 3d 901

[142] As in Seymour v. Colorado which now suggests that Googling an address within two weeks of a crime is sufficiently particular.

[143] Illinois v. Gates, *Supra.*

[144] United States of America, Plaintiff-appellee, v. Christopher A. Collins, Defendant-appellant, 830 F.2d 145 (9th Cir. 1987); Groh v. Ramirez, 540 U.S. 551 (2004); United States v. Grubbs, 547 U.S. 90 (2006)

[145] Including this space for which there is a reasonably likely chance that the suspect navigated at a time where few others would have can help circumvent issues of inaccuracy of available technology given the remote location.

abiding model, as it would generally need to meet a number of difficult requisites. First, the warrant's description for *where* to search would need to be limited in light of the number of users making queries per day with the technology being searched. While adding a timeframe would not by itself guarantee a remedy to this, it could help narrow the targets to just those who are reasonably likely to have made a specific query. Though what could be added to narrow the search area beyond this is difficult to say with any definitiveness, but some possibilities could include adding qualifiers, geolocation, or more specific terms.[146] As for *what* is to be searched, the keyword would need to be one that is not vague or general, and it would need to be incriminating enough as to establish a nexus between the location and the evidence of the information residing there (i.e. if there was a bank robbery then the query would have to incorporate details unique to the bank or the robbery itself without lowering the bar of suspicion). A possible search which would provide particularity would be if the keyword is one that has a high probability of concealing criminal intent and reveals very few individuals, say two or three. In this instance, so long as there is a high probability of the keywords concealing criminal intent, then there is no expectation of privacy as an individual holds no privacy interests on contraband.

[146] A geolocation parameter however would probably have very few use cases as many requisites would need to checked