**[FILL IN JURISDICTION]**

|  |  |
| --- | --- |
| [GOVERNMENT],  *Plaintiff*,  v.  [CLIENT NAME],  *Defendant*. | Case No. [FILL IN]  **MOTION TO SUPPRESS EVIDENCE FROM A KEYWORD WARRANT** |

# INTRODUCTION

[Client’s full name] files this motion to suppress [search engine] keyword evidence obtained using a modern-day general warrant in violation of the Fourth Amendment. The “keyword warrant” in this case allowed law enforcement to search and seize data belonging to [tens of/hundreds of—adjust to reflect what is known about how many people’s search engine queries were searched] millions of people who performed a [search engine] search for any one of the [insert number of search terms in warrant] terms during a period of [number] [hours, days, months]. [Client’s last name] had a Fourth Amendment interest in [her/his/their] internet search history, which contains an archive of intimate personal expression, and must be excluded because it is evidence obtained by an unconstitutional search. *See* *Mapp v. Ohio*, 367 U.S. 643 (1961).

Unlike a typical warrant for electronic information where a target is known and the warrant seeks the target’s data from a third party, a “reverse warrant” first identifies categories of data and then seeks information about people whose data falls into those categories. The warrant in this case followed this pattern. Law enforcement demanded that [search engine company] turn over information about [an untold number—here and below, adjust language if number is known or there is more specificity available] of its users, as part of law enforcement searching for a suspect to fit the crime. In sum, the keyword warrant here is an unconstitutional dragnet search that violates the Fourth Amendment because the search was too broad for the lack of probable cause, and it fails the Fourth Amendment’s particularity requirement. Further, [this/these] keyword warrant[s] impermissibly burden[s] [Client’s last name]’s rights under the First Amendment. Finally, the government’s keyword warrant[s] cannot be saved by the good-faith exception.

Throughout this brief, the term “keyword warrant” refers to a warrant that is served on a company that request the account information, Internet Protocol (“IP”) addresses, and other personal identification information the company has on users who search for specific terms within a specific time range. An [unspecified number] of users have their private data searched without any specific suspicion that they have done something wrong. Keyword warrants provide law enforcement with broad discretion to search and seize data about unspecified persons and thus violate the Fourth Amendment.

# BACKGROUND

## Alleged Facts of the Case

This motion is about a keyword warrant that [law enforcement organization] served on [search engine], in connection with [description of alleged crime]. At [time] on [date], [event] took place. [Description of events and/or alleged crime including dates, times, locations, and how and when law enforcement became involved].

[Preliminary details of law enforcement investigation, including background on whether law enforcement had investigatory leads other than the keyword warrant]. As discussed more below, law enforcement applied for, and received, a novel keyword warrant for the search and seizure of information about who searched on [search engine] for terms related to [event or location].

## Keyword Warrant Process

[Use the following arguments if your client’s information was given to law enforcement by Google. We have also seen warrants served to Microsoft and Yahoo, though Google is the search engine we know the most about. If the warrant was served to a company other than Google, you will need to do research into the specifics of how those platforms collect, store and track user information. For Google, this has included subpoenaing the company and seeking extensive discovery from the government, so there are sample requests that can be tailored to your client’s case.]

Warrants are served on Google via the Law Enforcement Request System website. Google holds an immense amount of power over what warrants it will and will not fulfil. According to Google, “requests must specifically name the product/service and identify the accounts by email address or another appropriate unique identifier. Requests to identify users by real names or IP addresses may be declined.” Google, *Serving Civil Subpoenas or Other Civil Requests on Google* (last visited May 10, 2022).[[1]](#footnote-2) Not much is known about how or how many keyword warrants are executed by Google because the process is generally carried out by law enforcement and Google away from public view and with little court oversight.

Google has indicated that it requires law enforcement to obtain warrants before it will carry out a search like the one that happened in this case. [CITE – this assertion can be found in ¶¶ 2–3 of the *Seymour* draft declaration from Nikki Adeli]. Google asserts that it requires such warrants to be “specific and narrowly tailored to reveal information connected to the alleged crime under investigation.” [CITE – this quote can be found in ¶ 3 of the *Seymour* draft declaration from Nikki Adeli]. Further, it describes a “staged process” for executing keyword warrants, which is described below. [CITE – this quote can be found in ¶ 3 of the *Seymour* draft declaration from Nikki Adeli].

During the first stage, upon receiving a keyword warrant, Google “creates a text-based query (that can include letters, numbers, or characters” based on the keyword search terms identified in the warrant. [CITE – this quote can be found in ¶ 4 of the *Seymour* draft declaration from Nikki Adeli]. That query is “run over the records of searches conducted through Google Search and Maps.” [CITE – this quote can be found in ¶ 4 of the *Seymour* draft declaration from Nikki Adeli]. This includes searches conducted by authenticated Google users and searches conducted in a way that is not associated with a particular Google account (e.g., a Google user is not logged into a browser, a person does not have a Google account, etc.). *See* [CITE – this assertion can be found in ¶ 6 of the *Seymour* draft declaration from Nikki Adeli]. Put another way, when responding to a keyword warrant, Google queries all searches run on Google Search or Google Maps, regardless of whether the person who conducted the search was logged into a Google account or consented to such use of their Google Search or Maps histories. As Google acknowledges, at the point the query is run, there is no way to know which users—if any—have used the keywords contained in the warrant. [CITE – this assertion can be found in ¶ 4 of the *Seymour* draft declaration from Nikki Adeli].

The query produces a set of results that reflects who searched for the terms identified in the warrant. [CITE – this assertion can be found in ¶ 5 of the *Seymour* draft declaration from Nikki Adeli]. Google then makes decisions about what information to include in its production to law enforcement. *See* [CITE – this assertion can be found in ¶ 5 of the *Seymour* draft declaration from Nikki Adeli]. Among those decisions, Google has indicated it frequently will disclose results that go beyond just the search terms mandated in the warrant. *See* [CITE – this assertion can be found in ¶ 5 of the *Seymour* draft declaration from Nikki Adeli]. It will do so even where the search results strongly imply that a keyword search is irrelevant. *See* [CITE – this quote can be found in ¶ 7 of the *Seymour* draft declaration from Nikki Adeli] (stating that Google will disclose search results for similar addresses in other cities or states).

Before turning over the query results to law enforcement, Google “de-identifie[s]” the results. [CITE – this quote can be found in ¶ 6 of the *Seymour* draft declaration from Nikki Adeli]. The “production version” of the query results “typically includes the following categories of information: (1) the date and time of the [keyword] search, (2) coarse location information inferred from the IP address from which the search was conducted, (3) the Query, (4) the Result, (5) the Host, (6) the Request, (7) a truncated Google identifier (known as the GAIA ID) if the search was conducted from an authenticated user’s account, or a truncated version of the Browser Cookie ID if the search was not conducted from an authenticated user’s account, and (8) the associated user agent string.” [CITE – this quote can be found in ¶ 6 of the *Seymour* draft declaration from Nikki Adeli]. “The Query” is the keyword a user enters into Google Search or Google Maps. “The Result” refers to the URL that is produced when a user conducts a keyword search and that shows the results of the search. “The Host” is [FILL IN]. “The Request” is [FILL IN]. The GAIA ID reflects [FILL IN]. And a “Browser Cookie ID” reflects [FILL IN].

While Google asserts that it de-identifies these results before disclosing them to law enforcement, *see* [CITE – this assertion can be found in ¶ 7 of the *Seymour* draft declaration from Nikki Adeli], the information provided can be used to identify people who used the relevant search terms without court supervision. As Google has explained, during the second stage of executing the warrant, law enforcement “can compel Google to provide additional information for those users the government has determined to be relevant to its investigation” if allowed by the warrant. [CITE – this quote can be found in ¶ 8 of the *Seymour* draft declaration from Nikki Adeli]. Separate from this, law enforcement can use a subpoena to obtain the name and address of the account holder. *See* [CITE – this quote can be found in ¶ 8 of the *Seymour* draft declaration from Nikki Adeli (stating that law enforcement can use subpoenas under 18 U.S.C. § 2703(c)(2) to obtain various categories of identifying formation after determining which accounts are relevant to the investigation)]. There is nothing in Google’s process that prevents law enforcement from seeking identifying information about all of the users identified in the de-identified query results.

## Keyword Warrant[s] in This Case

[Optional paragraph if the search engine refused to comply with earlier warrants from law enforcement:] On [date], the government submitted a keyword warrant to [search engine] requesting data about users who searched for variations of [term(s)]. [Search engine] refused to disclose data in response to this warrant. [Repeat prior sentences pursuant to the number of rejected warrants law enforcement provided to the search engine]. The government submitted a [second, third, fourth, etc.] version of the keyword warrant with which [search engine] complied.

Consistent with the first stage of a typical keyword warrant, on [date], the government requested data from [search engine] about users who searched [phrase(s)] between [time] and [time]. The government subsequently received [data particulars, e.g., anonymized identifiers associated with accounts, IP addresses, dates and times of searches, search histories, associated phone numbers and email accounts, etc.] from [search engine].

The results contained [what law enforcement was able to glean from data in relation to the investigation and your client].

Consistent with the second stage of a typical keyword warrant, on [date], the government requested [identifying information] from [search engine]. The request sought [identifying information particulars, e.g., full name, date of birth, telephone number(s), email address(es), physical address(es), all log-in IP address(es), location data associated with an account, the IP address with associated Port ID(s) used to register an account, internet search history, the contents of emails sent or received from an account, any other email address associated with an account, any photos or videos stored in connection with an account, etc.].

The government subsequently received [relevant information to the case at hand].

# ARGUMENT

The instant keyword warrant[s] constitute[s] a Fourth Amendment search under both the reasonable expectation of privacy and property-based frameworks. [It/These] [is an/are] unconstitutional general warrant[s] that lack[s] probable cause. Furthermore, [this/these] warrant[s] fail[s] the stringent particularity requirement that is attached to searches and seizures that raise First Amendment concerns. [Add the following sentence if the good faith exists in your jurisdiction:] Finally, the good-faith exception does not apply to the instant keyword warrant[s] because the warrant[s] lacked sufficient indicia of probable cause and it was facially deficient [insert additional good faith carve outs, if applicable].

## Accessing people’s internet search data constitutes a Fourth Amendment search.

Gathering data about an individual’s digital footprint can constitute a Fourth Amendment search. In *Carpenter*, the Supreme Court found that law enforcement’s acquisition of cell site location data constituted a search. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). Here, under either the reasonable expectation of privacy framework or a property-based theory of the Fourth Amendment, law enforcement’s collection of keyword search data was a search that violated the Constitution and must therefore be suppressed.

### Internet users have a reasonable expectation of privacy in their keyword search information because searches are private, expressive content.

The Fourth Amendment protects people from unreasonable searches and seizures of places and objects in which they have a reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Individuals have a reasonable expectation of privacy when (1) a person has exhibited an “actual (subjective) expectation of privacy,” and (2) that the expectation is “one that society is prepared to recognize as ‘reasonable.’” *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

The Court has recently expanded on how to determine a reasonable expectation of privacy in the context of new technology. In such cases, courts should look to “historical understandings” of what was unreasonable at the Founding, considering two guideposts: (1) the Fourth Amendment aims to secure “the privacies of life,” and (2) it prohibits surveillance that is too pervasive. *See Carpenter*, 138 S. Ct. at 2214. The Court has sought to preserve a “degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Consequently, the Court considers the “retrospective quality” of certain technology. *Carpenter*, 138 S. Ct. at 2218. If technology gives the government access to a category of information that would be “otherwise unknowable” before the digital age, that weighs in favor of finding a Fourth Amendment search. *See Carpenter*, 138 S. Ct. at 2218; *Riley v. California*, 573 U.S. 373, 393–94 (2014).

Keyword data reveals the privacies of life by exposing what people really think about, desire, and fear. *See* Seth Stephens-Davidowitz, *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are* 3 (2017). Keyword searches may reveal that someone hates their boss, they are the victim of domestic abuse, they are unhappy in their marriage, or they were recently diagnosed with cancer. *See* Stephens-Davidowitz, *supra*,at 6, 27. These details are intimate portraits of the inner workings of people’s minds. They reflect peoples’ concerns, hopes, and fears.

In many ways, this data is even more revealing than that at issue in *Carpenter*. There, the Court held cell-site location information (“CSLI”) disclosed the “privacies of life” to law enforcement because a cell phone “tracks nearly exactly the movements of its owner” as they travel “into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *See* *Carpenter*, 138 S. Ct. at 2217–18. Keyword search data exposes even more private information. Instead of tracking a person’s visit to a doctor’s office, keyword search data can expose a person’s medical diagnosis. Instead of following a person to a “potentially revealing” location, keyword search data explicitly reveals a person’s thoughts about any number of topics including things like race relations in the United States or their sexual orientation. *See* Stephens-Davidowitz, *supra*,at 6, 117. CSLI gives the government dots on a map through which it can make inferences about “familial, political, professional, religious, and sexual associations.” *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). By contrast, keyword search data gives the government explicit information about an individual’s innermost thoughts and associations. Brennan Ctr. for Justice, *Applying the Supreme Court’s Carpenter Decision to New Technologies* (Mar. 18, 2021).[[2]](#footnote-3)

[Incorporate caselaw specific to your jurisdiction here that supports the conclusion that the keyword warrant was a Fourth Amendment search].

Additionally, keyword search data reconstructs information that would have been unknowable to the government at the time of the adoption of the Fourth Amendment. In *Carpenter*, the Supreme Court highlighted that the same breadth and scale of CSLI surveillance would have been impossible when the Fourth Amendment was adopted. *See Carpenter*, 138 S. Ct. at 2218. It emphasized that the “retrospective quality” of CSLI gives law enforcement access to “a category of information otherwise unknowable,” given the pre-digital age limitations of records and “the frailties of recollection.” *See Carpenter*, 138 S. Ct. at 2218. Similarly, here, Google search terms are retrospective. A person’s search history is an inventory of all the names, addresses, terms, and questions about which they sought information. At the time the Fourth Amendment was adopted, this information would have been impossible to collect with the same degree of accuracy, comprehensiveness, and scale that current technology allows. This weighs in favor of finding that law enforcement’s search of [Client’s last name]’s search data was a Fourth Amendment search.

[Client’s last name] had a reasonable expectation of privacy in [her/his/their] keyword search data because it contains the privacies of life and it reflects information that was unknowable to law enforcement at the Founding. [This/These] warrant[s] [is/are] a Fourth Amendment search.

### The third-party doctrine does not apply to this data.

[Client’s last name] did not voluntarily convey [her/his/their] keyword search data to Google in a meaningful way, and thus did not meaningfully waive the privacy interest [she/he/they] [has/have] in [her/his/their] keyword search data.

The third-party doctrine is an exception to the Fourth Amendment that allows law enforcement to search the information of a person who has voluntarily given that information to a third party. However, the Supreme Court has since recognized that new technologies require a different approach to what constitutes voluntarily sharing information for third-party doctrine purposes. In *Carpenter*, the Supreme Court expressly distinguished the business records at issue in older third-party doctrine cases from location data collected by wireless carriers, holding that “there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.” *See* 138 S. Ct. at 2219;  *see also* *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (“A person [generally] has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties.” (emphasis added); *United States v. Miller*, 425 U.S. 435, 442 (1976).

Justice Sotomayor anticipated constitutional concerns with the invasive nature of digital searches of keyword data in *Jones*. She opined that the Fourth Amendment must evolve with changing technological realities because narrower understandings are “ill suited to the digital age.” *Jones*, 565 U.S. at 417. She went on to say that she “doubt[ed] that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.” *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring). Keyword warrants may be even more intrusive than the type of search Justice Sotomayor envisioned because they gather that type of internet search data on a scale that was previously impossible. Her concurrence was subsequently cited in the Ninth Circuit’s discussion of a person’s expectation of privacy in digital information that is not communications content but nonetheless reveals private information. *See* *United States v. Moalin*, 973 F.3d 977, 994 (9th Cir. 2020) (expressing doubt that warrantless collection of metadata comported with the Fourth Amendment). Courts across the nation recognize the need for heightened protection of digital information, including when companies aid people in managing their digital life.

Rulings on what digital information law enforcement has constitutionally collected under the third-party doctrine have been narrow, and do not apply to the data requested in the keyword warrant[s] here. Prior cases where IP addresses were considered publicly available information involve data that is substantially different from [Client’s last name]’s case because law enforcement targeted a specific user account, physical location, or email address when seeking the information from the third party. *See, e.g.*, *United States v. Soybel*, 13 F.4th 584, 587 (7th Cir. 2021); *United States v. Van Dyck*, 776 Fed. Appx. 495, 496 (9th Cir. 2019); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019). In those cases, *Carpenter* was found to not apply because the courts did not want to “call into question conventional surveillance techniques and tools.” 138 S. Ct. at 2220. The use of a pen register to collect non-content information about particular targets is distinctly different than the data collected by law enforcement here. Surveilling the search history of users is by no means conventional and, as discussed more below, the search conducted here targets many people beyond just [Client’s last name] without probable cause or particularity. Google does not connect its users to each other like phone companies or internet providers do, and thus *Smith*, *Miller*, and the IP address cases are inapposite.

Here, law enforcement wanted to search the private data of [tens/hundreds of millions] of users to potentially identify a person of interest. This clearly violates the Framers’ intent in adopting the Fourth Amendment, which was “to place obstacles in the way of a too permeating police surveillance.” *United States v. Di Re*, 332 U.S. 581, 595 (1948). If only the few who never need to consult a search engine for information could escape surveillance, then Supreme Court precedent and the Framer’s intent establish that this keyword warrant was an invalid search. *See* *Carpenter*, 138 S. Ct. at 2218 (relying on the fact that “only the few without cellphones could escape the tireless and absolute surveillance” in holding that obtaining historical CSLI constitutes a search).

There is no clear way for users to prevent their keyword searches from being captured by Google. The process outlined by Google indicates that the company will query the sum total of its records about what searches have been conducted on Google Search and Google Maps. [CITE – this quote can be found in ¶¶ 3, 6 of the *Seymour* draft declaration from Nikki Adeli]. If a user logs out of their account, their searches are still captured, retained by Google, and searched in response to keyword warrants. When a user is not logged in, the information is paired to a Browser Cookie ID rather than a GAIA ID, but it the search is still captured by Google and can be turned over to law enforcement. Indeed, in this case [fill this in with a description of how many (if any) keyword results were turned over to law enforcement that were not paired with a GAIA ID]. Because there is no way to prevent the collection of this data, [Client’s last name] cannot have meaningfully volunteered [her/his/their] search data to Google, and the third-party doctrine does not permit the government to intrude upon [Client’s last name]’s information.

### This is a search because users have a possessory interest in their keyword search data.

[Note: This interest has been analyzed with the assumption that the search engine implicated is Google. If the search engine implicated is not Google, you will need to heavily revise this section.]

Government conduct can also be a Fourth Amendment search if it involves an incursion into areas where someone has a property interest. [Client’s last name] and the [countless/millions/tens of millions/etc.] others whose information was collected in this reverse search have a property interest in the data law enforcement procured from Google because Google treats this kind of data as belonging to the user. Google’s Privacy Policy states that “across [its] services, [users] can adjust [their] privacy settings to control what [Google can] collect and how [the user’s] information is used.” *See* Google, *Privacy & Terms, Privacy Policy* (last visited Apr. 1, 2022).[[3]](#footnote-4) Google even recognizes that its users “expect Google to keep their information safe, even in the event of their death,” allowing a user to specify who can have access to their records after death, or in the alternative whether Google should delete the data. *See* Google, *Submit a Request Regarding a Deceased User’s Account* (2022).[[4]](#footnote-5) Account holders are also able to download their data and request that Google delete it at any time using the Google Takeout service, however Google Takeout does not give users the option to wholly opt out of data collection. *See* Google, *How to Download Your Google Data* (last visited Apr. 1, 2022).[[5]](#footnote-6) The Google Takeout webpage can only be accessed by users with a registered Google account. Google still collects the search history of people who use Google Search by identifying them by their web browser, and there is no ability for a person to delete that data once it has been collected. *See* Google, *Search History* (last visited Apr. 6, 2022) (showing users preference options for non-registered Google Search users and providing no option to prevent data collection or control data use once it has been collected).[[6]](#footnote-7)

When creating a Google account, users agree to provide Google with a license to use any content created by the user if that content is protected by intellectual property rights. Google, *Terms of Service* (last visited Apr. 1, 2022).[[7]](#footnote-8) The license gives Google the right to analyze user content to provide “recommendations and personalized search results, content, and ads.” *Id*. This provision implies that Google considers the words a user enters into the search bar to belong to the person who typed them, which Google is given permission to use via the license granted to Google upon account creation. There are seemingly infinite combinations of letters, words, and phrases that any person can put together when searching for something online, and according to Google’s terms of service, that person therefore has a property interest in whatever queries they create.

The fact that Google fulfills requests from government agencies when it has been issued process does not undermine a person’s property interest in the underlying data. Google sets forth clear circumstances under which it will hand over data to the government. For example, Google will disclose basic subscriber registration information and certain IP addresses pursuant to subpoena, non-content records pursuant to a court order, and contents of communications with a warrant. If Google reasonably believes that it can prevent someone from dying or from suffering serious physical harm, it may provide information to a government agency without the above documents. Google, *Privacy & Terms, Terms of Service* (last visited Apr. 1, 2022).[[8]](#footnote-9) But Google’s policies set forth a discrete set of circumstances in which it will disclose information to law enforcement, all of which imply that law enforcement has identified a known target and has obtained appropriate process to acquire the data, not that law enforcement will be permitted to conduct fishing expeditions without a known target. Google’s policies do not invite requests for the mass information dumps requested in keyword warrants.

Google provides users with several ways to exert control over how their data is accessed, though the average person may struggle to find and adjust these settings to fully exercise their control. [Client’s last name]’s [insert particulars of content acquired] constitutes [her/his/their] “papers or effects,” and cannot be searched or seized without a valid warrant. *See Soldal v. Cook Cty.*, 506 U.S. 62–64 (1992) (The Amendment protects the people from unreasonable searches and seizures of “their persons, houses, papers, and effects” . . . our cases unmistakably hold that the Amendment protects property as well as privacy). In a unanimous opinion, the Supreme Court recognized that “the expectation of privacy that comes from lawful possession and control and the attendant right to exclude would [not] differ” based on the circumstance of ownership. *Byrd v. United States*, 138 S. Ct. 1518, 1528 (2018) (citing to *Jones v. United States*, 362 U.S. 257 (1960)). Supreme Court precedent indicates that property becomes the effects of a person for Fourth Amendment purposes when they retain the right to exclude others from it, even if the property may be accessible by an outside entity. In the present case, Google has clearly structured its services to give users the ability to exclude anyone, including Google, from accessing their information.

[Client’s last name] thus retains the right to exclude others from [her/his/their] keyword search data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England \*2 (1771) (defining property as “that sole and despotic dominion . . . exercise[d] over the external things of the world, in total exclusion of the right of any other . . . .”); *Loretto v. Teleprompter Manhattan CATV Corp.,* 458 U.S. 419, 435 (1982) (calling the right to exclude “one of the most treasured strands” of the property rights bundle). This is not Google’s data; it is the users’ data that Google holds in trust. By collecting and searching [Client’s last name]’s keyword search data, law enforcement has denied [Client’s last name] the right to exclude others from [her/his/their] digital information. This violates the clear possessory interest [Client’s last name] has in this data, and thus a Fourth Amendment search occurred.

\* \* \*

People have both a reasonable expectation of privacy and a possessory interest in their keyword search data. Consequently, law enforcement’s acquisition of that data was a Fourth Amendment search. Furthermore, the third-party doctrine does not apply because [Client's last name] did not voluntarily convey [her/his/their] keyword search data to [search engine company].

## The instant keyword warrant[s] [is/are] unconstitutional.

The Fourth Amendment requires a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and (3) be issued by a neutral disinterested magistrate. *Dalia v. United States*, 441 U.S. 238, 255 (1979). When Fourth Amendment searches implicate First Amendment concerns, courts are careful to apply the Fourth Amendment’s requirements with “the most scrupulous exactitude,” mindful that “leaving the protection of [First Amendment] freedoms to the whim of the officers charged with executing the warrant” is unconstitutional. *Stanford v. Texas*, 379 U.S. 476, 485 (1965). If a warrant is invalid, the appropriate remedy is “ordinarily” to suppress the evidence derived from it in a criminal action. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

The instant keyword warrant[s] [is/are] the epitome of an indiscriminate, “dragnet-type law enforcement practice[],” sweeping up the search history data of [an untold number of people/millions/tens of millions/etc.] in the hopes of finding one potential lead. *United States v. Knotts*, 460 U.S. 276, 284 (1983). [This/These] [is a/are] general warrant[s]: [an] overbroad request[s] that fail[s] to meet the requirements of probable cause and particularity, and [is/are] antithetical to the Fourth Amendment. Because of the serious and significant First Amendment concerns raised by the search the government wanted to conduct, [this/these] warrant[s] must satisfy a “scrupulous exactitude” standard. *Stanford*, 379 U.S. at 485. The government failed to satisfy that requirement here. Due to the constitutional deficiencies of [this/these] warrant[s], the instant keyword warrant[s] [is/are] invalid under the Fourth Amendment.

### The instant keyword warrant[s] [is/are] [a] prohibited general warrant[s].

Keyword warrants pose the same threats as general warrants, or writs of assistance at the time of the Founding, “which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Riley*, 573 U.S. at 403. General warrants “specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.” *Steagald v. United States*, 451 U.S. 204, 220 (1981). Such is the case with [the] keyword warrant[s] here.

The prohibition of general warrants is a central tenet of American ideals; opposition to general warrants “helped spark the Revolution itself.” *Carpenter*, 138 S. Ct. at 2213; *see also* *Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481; *Marcus v. Search Warrant of Property*, 367 U.S. 717, 728 (1961). And general warrants are a key part of why the Fourth Amendment exists. *See* *Stanford*, 379 U.S. at 482–83 (describing the “battle for individual liberty and privacy” as won when British courts stopped the “roving commissions” given authority “to search where they pleased”). These warrants did not specify which houses to search or whom to arrest; “discretionary power [was] given to messengers to search wherever their suspicions may chance to fall,” leading to the destruction of property and the arrest of dozens of people. *Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763). General warrants left “the liberty of every man in the hands of every petty officer” and were ultimately denounced as “the worst instrument of arbitrary power.” *Stanford*, 379 U.S. at 481 (citation omitted).

Through the prohibition of general warrants, the government is restricted from such “arbitrary power.” *Stanford*, 379 U.S. at 481. By requiring sufficient probable cause and particularity, the Fourth Amendment sets restraints on searches and thereby limits the discretionary power of law enforcement. *See generally* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1298–1305 (2016) (describing the drafting process of the Fourth Amendment). For example, a warrant to search every house or pat down all people in a location would be unconstitutional. *See United States v. Glenn*, 2009 WL 2390353, at \*5 (S.D. Ga. 2009) (“The officers’ generalized belief that some of the patrons whom they had targeted for a systemic patdown might possibly have a weapon was insufficient to justify a cursory frisk of everyone present.” (quotation marks omitted)); *Commonwealth v. Brown*, 68 Mass. App. Ct. 261, 262 (Mass. App. Ct. 2007) (finding a warrant “authorizing a search of ‘any person present’ . . . resulted in an unlawful general search”); *Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (holding a “warrant to search all suspected places” for stolen goods was unlawful because “every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested”). But, with [a] keyword warrant[s] like the one[s] in this case, the government can do just that. It can search more than a home or pockets; it can search through users’ thoughts as expressed in searches, without particularized suspicion to search any particular user.

Keyword warrants represent precisely the sort of undirected, unrestrained search of constitutionally protected areas as reviled general warrants. When deciding if a search is constitutional, the Supreme Court has always been “careful to distinguish between [] rudimentary tracking . . . and more sweeping modes of surveillance.” *Carpenter*, 138 S. Ct. at 2215 (citing *Knotts*, 460 U.S. at 284). Keyword warrants result in the disclosure of many persons’ search history data and thus fall in the “sweeping” category about which the Supreme Court is most concerned. In *Knotts*, the Supreme Court cautioned against this exact kind of surveillance: “if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.” 460 U.S. at 283–84. The emergence of keyword warrants indicates that time is now.

Law enforcement did not—and could not—identify the individuals whose Google data was searched before conducting the search, and so necessarily failed to establish the requisite probable cause to search any one or all of them. As discussed further below, [this/these] keyword warrant[s] cannot meet the probable cause and particularity requirements of the Fourth Amendment, and thus [is an/are] invalid general warrant[s].

### The instant keyword warrant[s] lack[s] the requisite probable cause to justify such an overbroad search.

Keyword warrants are necessarily overbroad. By design, a keyword warrant does not specify the people or individual accounts to be searched because they are unknown. The explicit purpose is to search across potentially millions of user accounts to identify a subset of specific accounts that law enforcement would like to search further. The keyword warrant[s] here involved a search of every single [search engine] user from whom [search engine company] stores keyword search history. The search[es] here [was/were] a dragnet, conducted by [search engine company] at the government’s direction. Law enforcement commandeered [search engine company] to search through [millions/tens of millions/etc.] of private accounts, as well as the searches conducted by an untold number of users who were not logged into an account, to determine if any of them contained data of interest. The warrant[s] [was/were] unconstitutionally overbroad.

The Supreme Court has been clear that the scope of a search must be tailored to the probable cause in each case. Probable cause is “a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). And a warrant must be “no broader than the probable cause on which it is based.” *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Law enforcement must have “a reasonable ground for belief of guilt . . . particularized with respect to the person to be searched or seized.” *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Particularized probable cause “cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be.” *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). The breadth of a search must always match the probable cause.

Because keyword warrants include combing through the search history data of [an untold number/millions/tens of millions/etc.] of individuals in the hopes of finding one potential lead, they are an overbroad, “dragnet-type law enforcement practice.” *Knotts*, 460 U.S. at 284. Just like geofence warrants—which share dragnet qualities with keyword warrants—it is nearly impossible to conceive of a keyword warrant where only the perpetrator’s privacy interests are implicated. *See In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020). The scope of keyword warrants like [the one/those] in this case is unprecedentedly broad.

Keyword warrants produce data that reveal and intrude on intimate, constitutionally protected spaces such as the home. “At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his own home and there be free from unreasonable government intrusion.” *Silverman v. United States*, 365 U.S. 505, 511 (1961). In *Chatrie*, the court was “disturbed that individuals other than criminal defendants caught within expansive geofences may have no way to assert their privacy rights.” *Chatrie*, 2022 WL 628905 at \*17. Because keyword warrants cannot be—and [this/these] warrant[s] [was/were] not—appropriately scoped to the probable cause, many persons’ private information was obtained by law enforcement with no notice to those individuals. Those people “would seemingly have no realistic method to assert [their] privacy rights tangled within the warrant.” *Chatrie*, 2022 WL 628905 at \*18. These warrants “present the marked potential to implicate a ‘right without a remedy.’” *Chatrie*, 2022 WL 628905 at \*18 (quoting *Hawkins v. Barney’s Lessee*, 30 U.S. 457, 463 (1831)). People should be able to retreat into their homes and utilize search engines without fear that they will incur government scrutiny of those searches.

Here, however, the government did not have probable cause to search [tens of/hundreds of/etc.] millions of Google accounts and records about the searches conducted by an untold number of users who were not logged into an account. It did not have probable cause to search hundreds of accounts, dozens of accounts, or even one account. The government did not have probable cause to reveal the account information of [number, if known] of accounts.

Searching the same phrase potentially searched by the perpetrator of a crime does not, without more, give probable cause to search that person. Probable cause requires a logical “nexus” between the crime and the evidence to be seized. *See* LaFave, 2 Search and Seizure § 3.7(d) (6th ed. 2021). In contrast to warrants authorizing the acquisition of data about an individual suspected of a criminal offense, keyword warrants identify all [search engine] users merely due to the similarity of the terms and timing of their searches to a crime. A “person’s mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.” *Ybarra*, 444 U.S. at 91 (citing *Sibron v. New York*, 392 U.S. 40, 62–63 (1968)); *see also Di Re*, 332 U.S. at 587 (holding that a person does not lose their entitlement to immunities from search of their person because of their mere presence in a suspected car). This applies to digital searches as much as physical searches. A person’s mere digital propinquity (e.g., searching the same words or phrases), to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person. There is an abject absence of a “nexus” between the crime here and the indiscriminate seizure of search history records of an untold number of previously unidentified users.

The same is true regardless of if the government believes a keyword warrant is the only way to reveal the identity of the perpetrator of a crime. The government’s justification for probable cause in keyword warrants is backwards and has been recently rejected in analogous geofence cases. A federal court in Illinois rejected a geofence warrant application, finding the government’s position “resembles an argument that probable cause exists because those users were found in the place . . . [where] the offense happened,” an argument the Supreme Court rejected in *Ybarra*. *See In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020). The court further stated

[I]f the government can identify that wrongdoer only by sifting through the identities of unknown innocent persons without probable cause and in a manner that allows officials to rummage where they please in order to see what turns up, even if they have reason to believe something will turn up, a federal court in the United States of America should not permit the intrusion. Nowhere in Fourth Amendment jurisprudence has the end been held to justify unconstitutional means.

*In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754 (citation omitted). More recently in *Chatrie*, the court found “unpersuasive the United States’ inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person nearby.” *Chatrie*, 2022 WL 628905 at \*24. That inverted probable cause argument is the same in keyword warrants and similarly must be rejected.

From the outset, the government enlisted [search engine company] to search [untold/tens of/hundreds of] millions of unknown accounts, plus records about an unknown number of keyword searches conducted by people who were not logged into an account, in a massive fishing expedition. Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced [search engine company] to act as an adjunct detective, scouring the records of potentially millions of [Google Search and Google Maps] users to generate a lead for the government. In short, Step 1 compelled a search of the intimate, private data belonging to millions, in a digital dragnet that snared [number, if known] of accounts the data for which the government then seized—all without probable cause to search or seize data from a single account. Step 1 was fatally overbroad from the beginning. Following Step 1, the government lacked probable cause to search or seize the search history from a single account, let alone [number of accounts, if known, or “multiple,” if unknown or a small number].

There is an alarming lack of individualized suspicion for any, let alone all, of the individuals whose [search engine] data was searched under the warrant[s]. It would be near impossible to establish probable cause for the search history information of every [search engine] user who searched terms relevant to the crime here. The convenience of gathering search information on all of those individuals with a single warrant to [search engine company] does not obviate the requirements of the Fourth Amendment. *Riley*, 573 U.S. at 401 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)); *see also* *Carroll v. United States*, 267 U.S. 132, 153–54 (1925) (stating it would be “intolerable and unreasonable” to “subject all persons lawfully using the highways to the inconvenience and indignity” of a search just because some cars may contain contraband). When searching or seizing electronic data, the convenience of wholesale seizure of data for law enforcement also does not obviate the probable cause requirement. *United States v. Comprehensive Drug Testing, Inc.*,621 F.3d 1162, 1172–77 (9th Cir. 2010) (en banc) (per curiam). Thus, the instant warrant[s] [is/are] void for lack of probable cause.

Furthermore, the Supreme Court has held that judges should also consider whether there are First Amendment interests in the premises to be searched while evaluating the reasonableness of a warrant. For example, a warrant that would be sufficient to search an automobile may not be sufficient to search a news office because of the “independent values protected by the First Amendment” in the latter. *Zurcher v. Stanford* *Daily*, 436 U.S. 547, 569–70 (1970) (Powell, J., concurring). The keyword warrant[s] in this case involve[s] the search of many people’s internet search history, which is a unique venue that is intimately connected to First Amendment activity. People’s speech and association rights are exercised through keyword searches. Consequently, internet users’ interests in their search history weigh in favor of finding this warrant was overbroad.

[This/These] keyword warrant[s] [was/were] [an] overbroad search[es] without the requisite probable cause to search such a wide scope. There was an abject absence of individualized suspicion for every [search engine] user within the keyword warrant[s]. [This/These] warrant[s] [is/are] unconstitutional for lack of probable cause.

### The keyword warrant[s] in this case [is/are] not sufficiently particularized because [it/they] capture[s] people’s data who were not involved with the [alleged crime].

The Fourth Amendment requires that warrants “particularly describ[e] . . . the things to be seized.” U.S. Const. amend. IV. A warrant’s description of “what is to be taken” must leave “nothing . . . to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford*, 379 U.S. at 476. Thus, particularity requires that a warrant precisely spell out what is within its scope because law enforcement officers are prohibited from “seizure of one thing under a warrant describing another.” *Marron*, 275 U.S. at 196. A valid warrant must confine “the executing [officers’] discretion by allowing them to seize only evidence of a particular crime.” *United States v. Cobb*, 970 F.3d 319, 332 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). A valid warrant limits searches and seizures exclusively to evidence that is related to a designated crime. *See Andresen v. Maryland*, 427 U.S. 463, 481–83 (1976). Consequently, searching through a person’s data who has nothing to do with a designated crime is impermissible. The keyword warrant here violates the particularity requirement by allowing [law enforcement organization] and [search engine company] discretion to broadly search evidence unrelated to the [alleged crime at hand].

The warrant[s] here did not establish probable cause that is “particularized with respect to the person to be searched or seized.” *Pringle*, 540 U.S. at 371. The warrant[s] instead operated in reverse by requiring [search engine] to search and give law enforcement the data of *all* people who searched for [keyword search term at issue]. In *Chatrie*, the court found that a geofence warrant—another type of reverse warrant—lacked particularity because it captured the data of people who likely were not involved with the robbery in question. *Chatrie*, 2022 WL 628905, at \*44. The limitations of the geofencing technology meant that individuals were swept into the search who may have been at home in a nearby apartment complex or dining at a Ruby Tuesday restaurant. *Chatrie*, 2022 WL 628905, at \*44. Similarly, here, the keyword warrant[s] encompass[es] people who may have searched for [keyword search term at issue] to [get directions to an address, look up a person on social media, do research on deadly weapons, satisfy their curiosity about [topic], insert other innocuous reason for using the particular search term(s)]. The technical limitations of keyword warrants do not allow either Google or law enforcement to filter out people who searched specific terms for reasons unconnected to the [alleged crime at hand].

Additionally, the warrant[s] [is/are] not particularized because [it/they] [do/does] not particularly describe the digital data to be searched. While the government identified an address for [search engine company], [insert the search engine address referenced in warrant[s]], in the warrant application[s], warrants for searches of user data must particularly describe the digital account that will be searched, not simply the physical location where data is stored. Here, the keyword warrant[s] failed to specify which accounts and data could be searched.

Further, the warrant[s] here gave law enforcement and [search engine] too much discretion to search through [an untold number/millions/tens of millions/etc.] of users’ keyword data. Particularity requires a “detached” magistrate provide or confirm a description of who is to be searched and what is to be seized, instead of leaving it to the discretion of “the officer engaged in the often-competitive enterprise of ferreting out crime.” *Johnson v. United States*,333 U.S. 10, 13–14 (1948). This warrant gave law enforcement excessive discretion because it did not include [Insert specifics. Examples: language identifying which accounts law enforcement should obtain further identifying information about, *Chatrie*, 2022 WL 628905, at \*50, objective guardrails and benchmarks law enforcement could use to determine which accounts to further scrutinize, limiting the number of devices for which agents could obtain identifying information, a more restricted time period, narrower search terms, etc.].

[Use this paragraph if keyword terms implicate personal associations (e.g., addresses, person’s names, organizations)]. The particularity requirement is at its most stringent when items to be seized raise First Amendment concerns. *Stanford*, 379 U.S. at 485. The keyword warrant[s] here raise[s] First Amendment concerns because [it/they] expose[s] associations of people who searched for variations on [address, name, term]. The First Amendment protects the right to associate with others, in recognition that association advances a “wide variety of political, social, economic, educational, religious, and cultural ends.” *Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2382 (2021) (citing *Roberts v. United States Jaycees*, 468 U.S. 609, 622 (1984)). The Supreme Court has defended privacy in one’s associations under the First Amendment due to the “vital relationship between freedom to associate and privacy in one’s associations.” *NAACP v. Alabama*, 357 U.S. 449, 462 (1958). Internet users who searched for [term] to [get directions to a friend’s house, learn about a colleague, etc.] would have been swept up in this search along with users who searched for [term] for criminal purposes. The keyword warrant[s] here burden[s] bystanders’ freedom of association because disclosing associations to the government “can chill association even if there is no disclosure to the general public.” *Bonta*, 141 S. Ct. at 2388 (citing *Shelton v. Tucker*, 364 U.S. 479, 486 (1960)). [This/these] warrant[s] fail[s] to meet the heightened particularity threshold for warrants that raise First Amendment concerns.

[Use this paragraph if keyword terms implicate speech or communications (e.g., terms, questions, etc.) Note, if you are using this paragraph and the prior paragraph, both reference the same particularity precedent from *Stanford*.] The particularity requirement must be applied with “scrupulous exactitude” when items to be seized raise First Amendment concerns. *Stanford*, 379 U.S. at 485. The keyword warrant[s] here raise[s] concerns about First Amendment speech because [it/they] reveal[s] the personal communications of people who searched for [address, name, term]. The Sixth Circuit recognized that electronic communications play the same communicative role as more traditional forms of written expression. *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (“As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.”). Keyword searches are a form of private communication between the user and search engine. They are only intended to be viewed by the user because, like other communications, these searches can reveal deeply personal records of questions, thoughts, and fears. The Fourth Amendment has “an essential purpose” as a “guardian of private communication,” yet keyword warrants allow law enforcement to broadly collect private communications of bystanders. *Warshak*, 631 F.3d at 286.

Finally, there is also a “heightened sensitivity to the particularity requirement in the context of digital searches.” *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). The Second Circuit recognized that digital searches create “a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” *Galpin*, 720 F.3d at 447 (citing *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176). The warrant[s] here [is/are] a digital keyword warrant[s], which therefore adds another layer of necessity for the warrant to meet a heightened standard of particularity to be valid.

[This/These] [is a/are] general warrant[s]: [an] overbroad request[s] which fail[s] to meet the requirements of probable cause and particularity, antithetical to the Fourth Amendment. The instant keyword warrant[s] [is/are] [an] unconstitutional, invalid warrant[s]. The evidence from [this/these] warrant[s] must be suppressed.

## The good-faith exception does not apply.

[Note: The good-faith exception may not exist in your jurisdiction. If good-faith does not exist in your jurisdiction, you should cut this section and previous mentions of good-faith.]

The good-faith exception is limited to when law enforcement acts in good faith reliance on a warrant that is later found to be unconstitutional. Suppression is appropriate, and the good-faith exception does not apply, if the officers could not reasonably believe they had probable cause, or where a warrant is so facially deficient that no reasonable officer could have presumed it to be valid. *United States v. Leon*, 468 U.S. 897, 926 (1984). But, *Leon* states that the good faith exception does not apply in at least four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)); (2) where the judge acted as a rubber stamp for the police, *id.* (citing *Gates*, 462 U.S. at 288); (3) where a warrant affidavit lacks a substantial basis to determine probable cause*, id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid*, id.* at 923. [Based on the jurisdiction’s case law, there may be additional factors and reasons that are relevant and should be added.]

[It is recommended to analyze if, how, and why each of the *Leon* good-faith boundaries do or do not apply.] *First*, the good-faith exception does not apply because the keyword warrant was “so lacking in indicia of probable cause” to search [client’s information] that it was entirely unreasonable for any objective officer—i.e., one with even a rudimentary understanding of the Fourth Amendment’s requirements—to rely on it. *See Leon*, 468 U.S. at 923. Law enforcement must demonstrate a fair probability that the evidence they seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (4th Cir. 2011) (rejecting the good-faith exception where a warrant application contained “remarkably scant evidence . . . to support a belief that [the defendant] in fact possessed child pornography”); *see also* *United States v. Church*, 2016 WL 6123235, at \*6–7 (E.D. Va. Oct. 18, 2016) (observing that the good-faith exception was inappropriate where there was no evidence to connect the suspect’s house to the crime under investigation); *United States v. Shanklin*, 2013 WL 6019216, at \*9 (E.D. Va. Nov. 13, 2013). [Insert examples of good-faith cases in your jurisdiction that are in your favor.] That did not happen here. Rather, law enforcement obtained a warrant based on conjecture that [search engine company] had accurate search history data for accounts located near the crime scene before and up until the crime occurred. [The facts of your case may make the argument that law enforcement relying on, e.g., Google, for so much data is more compelling. Add those here to argue against good faith.] Obtaining warrants based on conjecture is certainly not “objectively reasonable law enforcement activity.” *See Leon*, 468 U.S. at 919. Thus, the good-faith exception must not apply in this case.

*Second*, the good faith exception does not apply because the keyword warrant was “facially deficient” and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. The warrant[s] [and supporting documents] [is/are] facially deficient because [insert aspects of warrant that are facially deficient]. [If there are unclear directions in the warrant(s) or in the supporting documents, add those aspects here]. Here, the warrant “was deficient in particularity because it provided no description of the type of evidence sought” and instead requested [insert broad request stated in warrant]. *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). [Jurisdictions generally have specific case law on limitations to the good-faith exception. If applicable, add those cases here.] Thus, the good-faith exception must not apply in this case.

[The third boundary of *Leon*—instances when probable cause cannot be determined from the substance of the warrant affidavit—is fact-dependent, and access to the warrant served to Google by law enforcement is needed to make this argument. If the warrant you are challenging is analogous to the examples listed, use the structure below as a foundation for your argument. There are two versions of a third boundary analysis below, please use the paragraph which is most analogous to your client’s case.]

[If your case is similar to the warrant requests approved in the Austin bomber case (i.e., the weapon or another item related to the crime is known, but there are no known suspects, include the following paragraph:] *Third*, to identify suspects, the government has requested the IP address, personal identifiable information, and user agent strings associated with Google account holders who searched for specific terms [and/or] addresses within a specific time-period. The government only limited the collection of users physically located in [location] according to their IP address [and/or] other Google account information in one of its requests. These criteria were based on conjecture from law enforcement that any potential suspects in this case would have a Google account and have searched for terms relating to the weapons used in the alleged crime. Obtaining warrants based on conjecture is not “objectively reasonable law enforcement activity.” *See* *Leon*, 468 U.S. at 919. Thus, the good-faith exception does not apply in this case.

[As an example, if your case is similar to the warrant requests approved in *Seymour* (i.e., cell phone found at the scene of the crime, but there are no known suspects, include the following paragraph:] *Third*, to identify suspects, the government has requested the IP address and personal identifiable information associated with Google account holders who searched for specific addresses within a specific time period. Law enforcement requested an anonymized list of devices that matched their initial search parameters, pursuant to Google’s refusing to fulfil warrants requesting more specific identifying information. However, the anonymized information included the IP addresses used by all accounts that are found to have conducted any of specified keyword searches. Once law enforcement searched the so-called anonymized list, it requested the personal identifiable information of several accounts which matched their initial search parameters. The final set of warrants served to Google requested to search, and if found, to seize immense amounts of personal information and data from three named suspects. These criteria were based on conjecture from law enforcement that any potential suspects in this case would have a Google account and have searched for terms relating to the [weapon used in/location of/etc.] the alleged crime. Obtaining warrants based on conjecture is certainly not “objectively reasonable law enforcement activity.” *See* *Leon*, 468 U.S. at 919. Thus, the good-faith exception does not apply in this case.

*Fourth*, the good faith exception does not apply because it is not reasonable for law enforcement to ever think such a sweeping dragnet privacy invasion is constitutional. And it cannot be the law that law enforcement gets to come up with new technological ways to do dragnet searches and courts will always apply good faith until a court specifically says that that specific version of a dragnet search is unconstitutional. If that is the case, then law enforcement will just continue to utilize different technologies to create new dragnet searches with no consequence. This is not reasonable. Any reasonable officer would recognize that no matter how you dress up a dragnet search, it is a dragnet search, which means it is unconstitutional. This principle was recognized long before people were able to carry highly advanced computers in their pockets. In *United States v. Tamura*, 694F.2d 591, 595–96 (9th Cir. 1982), the court held that “wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive and has been characterized as ‘the kind of investigatory dragnet that the fourth amendment was designed to prevent.’” (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)).

# CONCLUSION

Keyword warrants represent an unprecedented expansion of the government’s surveillance capabilities. *Carpenter*’s emphasis on the degree to which keyword search data obtained by law enforcement is sensitive or “deeply revealing” suggests that courts are recognizing the need to treat keyword search data differently from physical records. Based on the sensitivity of these records and the scope of the search, keyword warrants are Fourth Amendment searches of the unreasonable variety. The warrant[s] obtained in this case implicate[s] First Amendment concerns, and as such must withstand “scrupulous exactitude” under the Fourth Amendment. Yet this warrant cannot even survive the probable cause and particularity requirements under the Fourth Amendment. Instead [it/they] function[s] as [a] general warrant[s], not meeting the higher First Amendment standard. Finally, because the good faith exception cannot apply to a warrant no reasonable law enforcement officer would in good faith rely on, this keyword warrant is an unconstitutional search, and we request that its fruits be suppressed.

Respectfully submitted,

Date: [insert date] [insert signature block]

1. https://support.google.com/faqs/answer/6151275?hl=en#uscivil [https://perma.cc/J5AV-L2VE]. [↑](#footnote-ref-2)
2. https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age [https://perma.cc/LE8E-LHQZ]. [↑](#footnote-ref-3)
3. https://policies.google.com/privacy [https://perma.cc/9FDK-67YP]. [↑](#footnote-ref-4)
4. https://support.google.com/accounts/troubleshooter/6357590 [https://perma.cc/SY7D-LK95]. [↑](#footnote-ref-5)
5. https://support.google.com/accounts/answer/3024190 [https://perma.cc/TGZ3-LVAM]. [↑](#footnote-ref-6)
6. https://www.google.com/history/optout. [↑](#footnote-ref-7)
7. https://policies.google.com/terms?gl=US&hl=en [https://perma.cc/N4QE-MPLA]. [↑](#footnote-ref-8)
8. https://policies.google.com/terms/information-requests?gl=US [https://perma.cc/8T58-HZB5]. [↑](#footnote-ref-9)