UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID CHARLES RHINE, Defendant.	Criminal No. 21-CR-687 (RC) REPLY TO THE GOVERNMENT'S RESPONSE IN OPPOSITION TO MR. RHINE'S MOTION TO SUPPRESS EVIDENCE FLOWING FROM THE GEOFENCE WARRANT

The Court should reject the government's attempts to justify its geofence search here. First, the geofence queries were searches under the Fourth Amendment, and the Court should reject the government's attempt to re-write Fourth Amendment jurisprudence as protecting only "facts" one holds private. Second, the government repeatedly mis-states that the original warrant allowed it to search past copied location data, data that had been deleted by its owners, and compare it to the current Location History data. The warrant did no such thing. Rather, the government's reading of the warrant demonstrates the warrant's flaws—its lack of basic parameters to guide its execution. Third, the good faith exception does not save the government here. The government exceeded the scope of the warrant at step 1, and the warrant's lack of support for probable cause for the search conducted, and lack of particularity, render it a warrant that could not be relied upon in good faith. Finally, the Court should order an evidentiary hearing to resolve remaining disputed facts.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

I. ARGUMENT

A. The geofence search was indeed a search under the Fourth Amendment, and the Court should reject the government's argument to the contrary.

Even though it sought a multi-step warrant to conduct the geofence search here, the government argues that the geofence search was not actually a search under the Fourth Amendment. *See* Dkt. No. 59 at 11–25. As previously argued, the geofence search here was a Fourth Amendment search. *See* Dkt. No. 43 at 13–20. First, the government tries to overcome the obvious conclusion that a geofence search is, indeed, a search, by seeking a novel reading of the Fourth Amendment that is wholly unsupported by precedent. Second, the government mistakenly relies on third-party doctrine cases by mischaracterizing the nature and ownership of the items to be searched in this case. The Court should reject both of these arguments.

First, the government asks the Court to ignore *Carpenter v. United States*, 138 S. Ct. 2206 (2018), *Riley v. California*, 573 U.S. 373 (2014), *United States v. Jones*, 565 U.S. 400 (2012), and even *Katz v. United States*, 389 U.S. 347 (1967), to hold that the Fourth Amendment only protects "facts" that one hides from the world and offers no protection whatsoever in public places. The government argues, "The defendant cannot demonstrate a subjective expectation of privacy in the fact that he was inside (or around) the U.S. Capitol building in the afternoon of January 6, 2021[.]" Dkt. No. 59 at 12. In support of this contention, the government argues that the Capitol was a public place that was heavily surveilled, and that Mr. Rhine openly allowed others present to see him at the location at the time in question. *See id.* at 12–14. The government reasons that Mr. Rhine therefore had no Fourth Amendment-protected privacy interest in the *fact* of his location at the time in question. *Id.* at 14 ("Because the defendant lacked a legitimate expectation of privacy in his whereabouts near and within the U.S.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Capitol Building on January 6, he cannot assert a Fourth Amendment violation with respect to his location information at that location and time.").

This argument has no basis in controlling law. Well over 50 years ago, the Supreme Court rejected such an argument, explaining "the Fourth Amendment protects people, not places." *Katz v. United States,* 389 U.S. 347, 351 (1967). The question before the Court is not whether Mr. Rhine was in a public or private place, or whether he *otherwise* took efforts to conceal a particular fact. Rather, the question is whether the government infringed on a reasonable expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The government's invasion of privacy did not occur at the Capitol Building. It occurred when it compelled Google—a bailee of Mr. Rhine's personal data—to disclose to the government sensitive information about him and thousands of other users.

The Court has been clear that Fourth Amendment analysis must adapt with advancing technology.

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," . . . The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

Riley, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Among the deeply private information collected in cell phones about which the Court has expressed concern is location history. "Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." See *Id.* at 396 (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (SOTOMAYOR, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.")).

The Court also highlighted the Fourth Amendment concerns raised by cloud computing—that is, private data being stored in a server *not* held by an individual, but accessible to an individual via their personal device. *See* Riley, 573 U.S. at 397. Notably, the Court found, "Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." *Id.*

Applying these maxims, the Court plainly held that people have Fourth Amendment-protected privacy interests in their location data collected by their cell phones. *See Carpenter*, 138 S. Ct. at 2217. Indeed, this expectation of privacy exists *even if* a commercial provider generates or accesses the location data. *See id.* ("Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location."). This Court should reject the government's attempt to re-write precedent. Mr. Rhine did not voluntarily display his digital location data. As in *Carpenter*, Mr. Rhine had a Fourth Amendment-protected privacy interest in his digital Location History data.[1]

[1] Neither of the government's citations to district court decisions dealt with data similar to the data at issue here. *See* Dkt. No. 59 at 15. *Sanchez v. Los Angeles Dep't of Transportation*, 39 F.4th 548, 559 (9th Cir. 2022) concerned electric scooter companies' compliance with a city regulation designed to minimize clutter on public throughways by sharing with the local government real-time location information for the scooters the company owned. No user had exclusive use of any single scooter owned by the company such that their personal movements could be tracked by such data. Similarly, *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182 (N.D. Cal. 2020) involved a *private* invasion of privacy claim against Facebook (not the government), for collecting data on the IP address its users use to connect to the cite. Even in Fourth Amendment caselaw, IP addresses hold very different ground than location data collected about a person's whereabouts from their cell phones. Rather, IP addresses are the digital equivalent of license plates. Indeed, even the Court in *Heeger* explained

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Second, the government argues that Mr. Rhine voluntarily made his location history public under the third-party doctrine by agreeing to Google's terms of service. *See* Dkt. No. 59 at 14–25. However, this argument contradicts existing caselaw on similar user agreements. The government argues that because Google was *able* to and even had a *right* to access Mr. Rhine's Location History data, he had relinquished his expectation of privacy.

But even in *Katz*, the Supreme Court held that Mr. Katz had a reasonable expectation of privacy in his call from a public phone booth *even though* telephone companies at the time were able to and had a right to monitor calls to "protect themselves and their properties against the improper and illegal use of their facilities." *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967). As Justice Stewart later explained:

> A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."

Smith v. Maryland, 442 U.S. 735, 746–47 (1979) (STEWART, J., Dissenting) (quoting *Katz*, 389 U.S., at 352).

The government asks this Court to reject prior caselaw and instead rest a person's Fourth Amendment rights on the terms of a contract—and a notoriously misleading contract of adhesion at that. *See* Dkt. No. 43 at 18–19. Rather, the Court plainly held in *Carpenter* that contract terms do not dictate whether a person has voluntarily shared information or items with a third party. The proper question is

---

"The collection of IP addresses is a country mile from the CSLI data collected in *Carpenter*[.]" *Id.* at 1190.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

whether in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. 138 S. Ct. at 2220; *see also United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018) (recognizing that the terms of a rental car contract do not determine a driver's reasonable expectation of privacy). In the case of Location History, Google's pop-ups and terms of service do not suffice to extinguish users' privacy interest in their account data.

Location History is also not a business record, as the government suggests. *See* Dkt. No. 59 at 14–17. The Sixth Circuit aptly explained the difference between information voluntarily conveyed to a business to conduct a transaction, (the "business record" examined in *United States v. Miller*, 425 U.S. 435 (1976)), and digital information owned by users and merely stored and conveyed by a business:

> First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. [] Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." [] By contrast, Warshak received his emails through NuVox. NuVox was an intermediary, not the intended recipient of the emails.

United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (quoting *Miller*, 425 U.S. at 443) (citing Patricia L. Bellia, Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 165 (2008) ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests.")). Thus, *Miller* is not controlling.

Indeed, Google users reasonably understand that their Location History *belongs to them*, not to Google. *See* Dkt. No. 43 at 21–22. Users' property (data) may be stored on Google servers and users may have granted Google some access to their data. But

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

limited expected access by Google does not eliminate users' reasonable expectation of privacy against wholesale intrusion into and dissemination of this data.

Indeed, the trespass-based Fourth Amendment protections (which *Katz* supplements) plainly protect property owners against intrusions onto such property *beyond* those entrances onto their property that they reasonably permit. *See Collins v. Virginia*, 138 S. Ct. 1663, 1671 (2018) (police intrusion onto driveway to lift tarp and identify a vehicle violated the Fourth Amendment); *Florida v. Jardines*, 569 U.S. 1, 8–9 (2013) (police violated Fourth Amendment by bringing trained police dog to do an investigatory sniff of person's front porch); *United States v. Jones*, 565 U.S. 400, 404–05 (2012) (Fourth Amendment violation when police installed a GPS tracking device on a person's vehicle) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

Indeed, the trespass-based protections of the Fourth Amendment affirm that people maintain a reasonable expectation of privacy in their property *even if* they afford a limited license for some to intrude on that property in certain ways or for certain purposes. For example, in *Jardines*, the Court recognized that people implicitly permit others to intrude onto their curtilage (there, their front porch) in limited manner and for limited purposes: "This implicit license typically permits the visitor to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave. Complying with the terms of that traditional invitation does not require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters." *Jardines*, 569 U.S. at 8. However, "introducing a trained police dog to explore the area around the home in hopes of discovering incriminating evidence is something else. There is no customary invitation

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

to do that." *Id*. at 9. Ultimately, "[t]he scope of a license—express or implied—is limited not only to a particular area but also to a specific purpose." *Id*.

So too here, even if a user *understood* Google's terms of service, such terms allow Google the limited ability to access and store a user's Location History data, *subject to the user's ability to delete that data when they choose*. Google, *Manage Your Location History*, *supra*. And the purpose of this access is to improve users' experiences and to allow them to access features, such as maps. Nothing in the purported license relinquishes a user's expectation that parties *other than* Google would intrude upon their property, or that Google would intrude upon their property for another purpose.

Just like any rented or borrowed physical space, so too a rented or borrowed digital space is entitled to Fourth Amendment protections. Even though renters may be aware that owners and their agents may regularly access their space, they do not relinquish their expectation of privacy in the space as to all intruders. *See Warshak*, 631 F.3d at 287 (citing cases holding hotel guests and tenants still maintain Fourth Amendment expectations of privacy despite regular third-party access to their space) ("That expectation persists, regardless of the incursions of handymen to fix leaky faucets. Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question."). Both *Katz*'s reasonable expectation of privacy test and the pre-existing trespass test for Fourth Amendment protection affirm that the geofence search here was, indeed, a search.

B. The good faith exception does not apply—the government was on notice that it was conducting a Fourth Amendment search of alarming breadth, and suppression is appropriate.

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is based on "objectively reasonable law enforcement activity."

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

But, *Leon* "good faith" offers no qualifications in 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 *Illinois v. Gates*, 462 U.S. 213, 288 (1983)); (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.

The Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id*. at 917, 923. The *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was void *ab initio*. As set forth previously, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). But, even if the Court determines that *Leon* applies here, two of the firm boundaries to the good faith rule that *Leon* recognizes clearly apply.

First, the good faith exception should not apply because the government exceeded the scope of the warrant when executing it. The good faith exception in *Leon* applies "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." 468 U.S. at 920. However, here, the government did not act within the scope of the warrant. Rather, at step 1, the government exceeded the scope of the warrant. Rather than simply accepting Google's responsive lists from its Location History database regarding accounts pinging within the geofence during the time periods delineated in the warrant, the government also impelled Google to produce lists of accounts in separate data—Location History

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

strategically preserved on an earlier date even though users had subsequently deleted or disabled their Location History. This was *not* authorized by the Part 1 warrant. *See generally* Ex. A.[2]

Notably, the warrant impelled Google to search its "Location History data" to assemble three lists requested by the government—the geofence time window list, and the two "control" window lists (at noon and 9:00 p.m.). *Id.* at 4, 6. However, Location History data is a fluid dataset—it is not any historical record that Google may keep without its users' knowledge or agreement. By Google's own definition, any user may "control what's saved in your Location History. You can view the places where you've been in Google Maps Timeline, which you can edit or use to delete your Location History." Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687?hl=en (last visited Dec. 5, 2022). Rather than simply executing the warrant as written—compiling the three requested lists from the dataset—the government exceeded its bounds. The government *also* searched *other* Google records of historical copies of the data set[3] to examine the Location History of accounts where users had actually disabled or deleted their location history—indicating their intent that their bailee cease storing these records. In other words, the government searched *other* records held by Google to identify actions taken by users wholly outside of the geofence parameters—namely, to identify users who deleted their location history or Google accounts fully after the geofence time window. The government's disregard for the terms of the warrant removes this case from *Leon*'s good faith exception.

---

[2] Without reciting any relevant language—indeed, none exists—the government claims the Part 1 warrant *did* authorize such a search. *See* Dkt. No. 59 at 30.

[3] The government seems to argue, without explicitly explaining its position, that this search was included within the warrant's request to search Google "Location History data." As discussed below, such interpretation emphasizes the lack of particularity in the warrant.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Second, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search thousands of users' data that it was entirely unreasonable for any objective officer to rely on it. *See Leon*, 468 U.S. at 923. "'Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.'" *Id.* at 915 (1984) (quoting *Gates*, 462 U.S. at 239).

Here, the government argues that "the warrant articulated probable cause to believe that every person in the U.S. Capitol building at the time of the siege had either engaged in or witnessed criminal activity." Dkt. No. 59 at 28. Indeed, in the warrant affidavit, the government sought subscriber information where there was a 68 percent chance (assuming Google was meeting its accuracy goals) the subscriber's device was within the Capitol Building between 2:00 p.m. and 6:30 p.m. on January 6, 2021. *See* Ex. B at 6–7. The government's affidavit did not assert that every person present at the Capitol had committed a crime, but rather asserted only that the information sought may identify "individuals who were in close proximity to the area of the target offense." Ex. A at 19. Even if accepted, this argument acknowledges that not every account in the geofence area was believed to belong to a person who engaged in criminal activity. The government seeks to save its exceedingly broad search by arguing that even innocent devices "were likely to contain evidence documenting the crimes of others on January 6." *Id.* at 36. There may be evidence that *some* people present were using cell phones, but there was not evidence that *every* person was, nor, that every person was capturing evidence of crimes (for example, taking videos or photos). Still, the government searched the Location History and subscriber information of thousands of people.

The Supreme Court has time and again emphasized the extremely personal nature of cell phone information, location data, and digitally stored information. *See Riley*, 573 U.S. at 403, *Carpenter*, 138 S. Ct. at 2217–18 (2018). No reasonable law

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

enforcement officer would conclude that an invasive search of this information for thousands of people—not all of whom are actually suspected of criminal activity nor of preserving evidence of such—is legal.

Furthermore, in the Step 2 warrant, the approving court authorized the search of subscriber information—a highly invasive search—based on the conclusory claim by the agent requesting the warrant: "Based on my knowledge, training, and experience, I know that criminals will delete their Google accounts and/or their Google location data after they commit criminal acts to protect themselves from law enforcement." Ex. B at 8. Such conclusory claim is not supported by a single factual claim. Indeed, the facts claimed—that a small fraction of those accounts identified within the geofence window appeared to have deleted their accounts or location history—*contradicts* the claim that such deletion is evidence of criminal activity. Rather, as previously argued, a person may delete their Location History or Google account for a variety of benign reasons.

Even if a deletion *were* intended to avoid police involvement, courts have repeatedly rejected actions to avoid police as a basis for probable cause. *See, e.g.*, *Florida v. Bostick*, 501 U.S. 429, 437 (1991) ("We have consistently held that a refusal to cooperate, without more, does not furnish the minimal level of objective justification needed for a detention or seizure."); *Florida v. Royer*, 460 U.S. 491, 497–98 (1983) (a person's "refusal to listen or answer does not, without more, furnish those grounds [to seize/detain them]."); *Wong Sun v. United States*, 371 U.S. 471, 484 (1963) ("it is a matter of common knowledge that men who are entirely innocent do sometimes fly from the scene of a crime through fear of being apprehended as the guilty parties, or from an unwillingness to appear as witnesses. Nor is it true as an accepted axiom of criminal law that 'the wicked flee when no man pursueth, but the righteous are as bold as a lion.'") (quoting *Alberty v. United States*, 162 U.S. 499, 509 (1896)). This "mere ratification of the bare conclusions of others" to find probable cause for subscriber

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

information from apparently deleted accounts could not have been relied upon in good faith. *See Leon*, 468 U.S. at 915. It was unreasonable for any law enforcement officer to accept this finding of probable cause as legitimate when it relied on the unsubstantiated assumption that anyone who removes Location History, or their Google account must be involved in criminal activity.

Third, the good faith exception does not apply because the warrant here was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923. "[I]t is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607–09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases).

Here, the warrant lacked basic particularity as to both the items to be searched and to be seized (or turned over). First, the warrant identifies the place to be searched as Google's Location History data and subscriber information. *See* Ex. A at 4. Further, the warrant indicates that Google must use "Location History data" to assemble the three lists of account holders to be turned over to the government. As discussed above, the government went beyond the actual Location History data to search other records maintained by Google. If the Court accepts the government's argument that these expansive searches complied with the warrant, such finding underscores the warrant's lack of particularity. The government's reading suggests that the warrant authorized the government to search any record held by Google where Location History data or subscriber information was present. This reading lacks clarity, and demonstrates the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

warrant's flaws, inviting a near limitless search of most records held by Google about its users.

The government also asserts that the warrant's list of items to be seized enhanced its particularity. Dkt. No. 59 at 36–37. However, the government's own reading of what that list meant undermines its argument. The list of items to be seized included, at Step 1, *only* the three lists of accounts specified—the geofence window list, the noon control list, and the 9:00 p.m. control list. *See* Ex. A at 6. Yet, the government at Step 1 actually obtained additional lists—lists from other records held by Google about accounts that may have been within the geofence during the relevant window. The warrant's lack of particularity for Step 2 invited this overreach. The warrant stated that, after receiving the three lists, "The government will then review these lists in order to identify information, if any, that is not evidence of crime (for example, information pertaining to devices moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case)." Ex. A at 6. This *included* removing the control lists from the geofence window list, but did not include any other particularized narrowing mechanisms. *Id.*

The government indeed employed a search in excess of the warrant to invade other records held by Google and to identify actions taken by account holders *outside* of any of the time periods identified in the warrant (namely, to identify changes made to an account holder's Location History settings *after* January 6). The government argues that the warrant was facially reasonable because the approving court "reviewed and approved the criteria subsequently used to narrow the devices for which subscriber information was seized." Dkt. No. 59 at 35. However, this "approval" of the government's overreach and apparent unfettered access to private data held by Google *outside* the bounds of the Part 1 warrant demonstrates the warrant's facial invalidity. No

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

reasonable law enforcement officer would expect a neutral and detached court to reward a law enforcement search in excess of the terms of a warrant.

The government cannot argue it did not understand how this warrant would work because the basic contours of a geofence warrant came from repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018. Ex. E at 456–57 ("CCIPS is an agency that . . . our counsel engages with to discuss sort of certain procedures that may be relevant for the way that . . . Google will need to handle these types of requests"); *id.* at 476 (noting repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *id.* at 552-53 (law enforcement confirming standardized language tools for geofence warrants). For any of these reasons, the Court cannot find that the good faith exception applies to evidence obtained from the geofence warrant here and the fruits flowing therefrom.

C. The Court should hold an evidentiary hearing to resolve remaining disputes of fact.

The government's primary disputes with Mr. Rhine's motion to suppress the fruits of the geofence warrant, including the later search of his home and cell phone, are factual. *See* Dkt. No. 59 at 40–43. The government has offered no new evidence to support its requested inferences from the evidence as opposed to Mr. Rhine's. As such, the Court should hold an evidentiary hearing to resolve these disputes of fact.

II. CONCLUSION

The Court should reject the government's attempts to justify its invasion of the private data of Mr. Rhine and thousands of other people. The Court should hold that the geofence search here violated the Fourth Amendment and should suppress the fruits of that search. As this case demonstrates, coming on the heels of numerous government geofence searches, suppression is necessary to deter the government from continuing to

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

conduct digital dragnets—the modern equivalent of the general warrants the Fourth Amendment intended to stop.

DATED this 7th day of December 2022.

Respectfully submitted,

s/ Rebecca Fish
s/ Joanna Martin
Assistant Federal Public Defenders

Attorneys for David Charles Rhine

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710