

1 Manohar Raju  
2 Public Defender  
3 San Francisco Public Defenders Office  
4 Matt Gonzalez  
5 Chief Attorney  
6 Sierra Villaran, SBN 306949  
7 Deputy Public Defender  
8 555 Seventh Street  
9 San Francisco, CA 94103  
10 (415) 575--819  
11 Sierra.Villaran@sfgov.org

12 Michael Price (*pro hac vice*)  
13 Litigation Director, Fourth Amendment Center  
14 National Association of Criminal Defense Lawyers  
15 1660 L Street, NW, 12<sup>th</sup> Floor  
16 Washington, DC 20036  
17 (202) 465-7615  
18 mprice@nacdl.org

19 Attorneys for LaQuan Dawes

20 **Superior Court of the State of California**  
21 **County of San Francisco**

22 **People of the State of California,**

23 Plaintiff,

24 vs.

25 **LaQuan Dawes,**

26 Defendant.

27 Court No: 19002022

28 **Reply to State's Opposition to  
Defendant's Motion to Quash and  
Suppress Evidence**

Date: September 17, 2021

Time: 9:00 AM

Dept: 20

29 LaQuan Dawes, through counsel, replies as follows to the State's opposition to Mr. Dawes'  
30 motion to quash and suppress a "geofence" warrant issued on December 4, 2018. *See* People's  
31 Opp. to Def. Mot. to Quash & Suppress Evidence at 1 ("Opp."). This matter is currently set for  
32 September 17, 2021, for the limited purpose of determining whether Mr. Dawes had a reasonable  
33 expectation of privacy in his Google Location History data. If the Court finds that he did, then it  
34 will not be necessary for Mr. Dawes to enforce a subpoena issued to Google seeking, *inter alia*,

1 information about the process of enabling the “Location History” service.<sup>1</sup> Accordingly, Mr.  
2 Dawes limits this reply to explaining why he had a constitutional privacy interest in his Location  
3 History data, and why the State’s arguments to the contrary fall flat.

#### 4 **Introduction**

5 This case involves a novel and invasive form of electronic surveillance, a “geofence”  
6 warrant, used here to generate suspects in a burglary investigation. The warrant required Google  
7 to search the contents of *every single Google user account* with Location History enabled,  
8 totaling “numerous tens of millions” of people. Decl. of Marlo McGriff at 4, *United States v.*  
9 *Chatrie*, No. 3:19-cr-00130 (Mar. 11, 2020) (Def. Exhibit A). The warrant did not specify the  
10 names or accounts of any of the individuals whose information was to be searched or seized.  
11 Instead, the State enlisted Google to comb through a massive trove of private data and hand over  
12 the results to the San Francisco Police Department. The State then used the seized data to  
13 identify Mr. Dawes as a suspect in the burglary.

14 Mr. Dawes has moved to quash the search warrant and suppress the resulting evidence,  
15 arguing that the warrant was profoundly overbroad and lacking particularity—in effect, an  
16 unconstitutional general warrant. *See* Mot. to Quash & Suppress Evidence at 1-2, 10-12. The  
17 State’s counterargument is that there was no “search” at all because Mr. Dawes did not have a  
18 privacy interest in his Location History data. Opp. at 6. The State offers two points in support: 1)  
19 the data covered “less than four hours,” and (2) Mr. Dawes consented to its collection and  
20 disclosure to law enforcement. Opp. at 5-7. The State is wrong on both the law and the facts.

21 First, there is no *de minimis* exception to the Fourth Amendment. Mr. Dawes enjoys a  
22 reasonable expectation of privacy in his Location History data following the Supreme Court’s

---

23 <sup>1</sup> Mr. Dawes understands that the September 17<sup>th</sup> hearing, as well as this round of briefing, is  
24 confined the question of whether he had a reasonable expectation of privacy in his Location  
25 History data. Mr. Dawes maintains Google possesses unique information about the process of  
26 enabling Location History is important to answering this question. And as a result, Mr. Dawes  
27 has subpoenaed Google for that information. But should this Court determine that the record is  
28 sufficient to find a privacy interest in this data, then Mr. Dawes would have no need to seek  
further information from Google. In that event, Mr. Dawes would, however, ask this Court for  
the opportunity to fully respond to the State’s arguments regarding the warrant’s overbreadth,  
lack of particularity, and absence of good faith, prior to any suppression hearing or determination  
on the merits.

1 landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and *United States v.*  
2 *Jones*, 565 U.S. 400 (2012), as well as under *Kyllo v. United States*, 533 U.S. 27 (2001) and  
3 *United States v. Karo*, 468 U.S. 705 (1984). *Carpenter* and *Jones* recognized a privacy interest in  
4 GPS data and cell site location information (“CSLI”), both of which are at issue in this case. *See*  
5 *Carpenter*, 138 S. Ct. at 2217; *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring), *accord*  
6 *Carpenter*, 138 S. Ct. at 2215. And while the shortest search in either opinion involved *seven*  
7 days of CSLI (not 129) for a single individual, *see Carpenter*, 138 S. Ct. at 2217, the Court’s  
8 reasoning applies with at least equal force, if not more, to the facts here.<sup>2</sup> This is because  
9 Location History data is far more precise than the cell tower data at issue in *Carpenter*. Precision  
10 matters because Location History data is more *potent* than CSLI. A single data point from CSLI  
11 may reveal which neighborhood or zip code a device is in. By contrast, a single Location History  
12 data point may have GPS-level accuracy, pinpointing a device’s specific location at any moment  
13 in time. A little goes a long way; Location History can reveal the same kind of private  
14 information with just a far fewer data points.

15 Second, as a factual matter, Mr. Dawes did not consent to enabling Google’s Location  
16 History service on his account. Rather, it appears to have been enabled without warning and by  
17 default when Mr. Dawes set up a new cell phone in 2015 running Google’s Android operating  
18 system. Mr. Dawes has retained a digital forensics expert, Spencer McInville, who has reviewed  
19 the account audit logs provided by Google and prepared a report and video concluding that  
20 Location History was “automatically activated at device set up with no user consent requests.”  
21 *See* Report of Spencer J McInville (Sept. 10, 2021) (Def. Exhibit B); McInville, Cell Phone  
22 Setup Video (Sept. 10, 2021) (Def. Exhibit C). Nonetheless, the State asserts, without evidence,  
23 that Mr. Dawes “expressly agreed” to a 2018 Google Privacy Policy, three years after the service  
24 was enabled on his account, which somehow eliminated any privacy interest in his physical  
25 location at all times. *Opp.* at 7. The Supreme Court has repeatedly declined to define Fourth  
26 Amendment rights based on such policies, and in any event, the 2018 policy was plainly

27 \_\_\_\_\_  
28 <sup>2</sup> In fact, the government’s demand for seven days of data in *Carpenter* netted only two days of  
data. *See* 138 S. Ct. at 2212.

1 insufficient to make any consent informed, meaningful, or voluntary. Instead, the Supreme Court  
2 has consistently looked beyond such ephemeral and inscrutable policies to consider context,  
3 common sense, and the sensitivity of the data instead.

4 Even if Mr. Dawes had intended to enable Location History, he would still enjoy a  
5 reasonable expectation of privacy in it for two reasons. First, the so-called “third-party” doctrine  
6 does not apply to Location History data. The State relies on two cases from the 1970s to contend  
7 otherwise, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735  
8 (1979). These cases, however, rest on outdated assumptions that do not translate into the digital  
9 age. The third-party doctrine is not on solid footing when it comes to digital searches and  
10 seizures, and the State’s attempts to argue to the contrary are similarly out of touch and  
11 unpersuasive. This is especially true because Location History records can precisely locate  
12 people inside of their homes and other constitutionally protected spaces, which constitutes a  
13 search for that reason alone under *Kyllo* and *Karo*. Second, the State of California recognized a  
14 privacy interest in mobile location data when it enacted the 2016 California Electronic  
15 Communications Privacy Act (CalECPA) and declined to extend the third-party doctrine to  
16 excuse the warrant requirement. CalECPA protects Location History data and is strong evidence  
17 that Mr. Dawes had a reasonable expectation of privacy in it.

#### 18 **Argument**

#### 19 **1. Mr. Dawes Had a Reasonable Expectation of Privacy in His Location History Data.**

20 Mr. Dawes had a reasonable expectation of privacy in his Location History records. He had a  
21 privacy interest in them under the Supreme Court’s reasoning in *Carpenter* and *Jones* because,  
22 like CSLI and GPS data, Location History also reveals the “privacies of life.” *Carpenter*, 138 S.  
23 Ct. at 2214. Although this case involves a shorter duration of data, the precision and always-on  
24 nature of Location History makes it even more invasive, requiring less to achieve the same  
25 effect. Indeed, just a small amount of Location History can identify individuals inside of their  
26 homes and other private spaces. And as a result, a geofence warrant almost always involves  
27 intrusion into these constitutionally protected areas, infringing on the property-based privacy  
28 interests recognized by the Court in *Karo* and *Kyllo*.

1           **A. Location History Is At Least As Precise as CSLI, Often Has GPS-Quality**  
2           **Accuracy, and Is Highly Intrusive.**

3           As the State concedes, Location History is at least as precise as CSLI, Opp. at 6., but it can  
4 also be as accurate as GPS. The reason for this variation is because Google uses multiple data  
5 sources to estimate a user’s location, including CSLI and GPS, as well as Wi-Fi and Bluetooth,  
6 which vary in their accuracy. Def. Ex. A at 4. In this case, all the estimated Location History  
7 points derive from either Wi-Fi or GPS signals, which Google states are “capable of estimating a  
8 device’s location to a higher degree of accuracy and precision than is typical of CSLI.” *Id.*  
9 Additionally, 56% of the data points derive from the same type of GPS signals at issue in *Jones*,  
10 which can be accurate to less than a meter. *See* Hr’g Tr. at 18-20 Mar. 4-5, 2021, *United States v.*  
11 *Chatrie*, No. 3:19-cr-00130 (Def. Exhibit D). At the same time, Location History can do things  
12 that even GPS cannot do, like determine a user’s elevation and identify the specific floor of the  
13 building they are on. *Id.* at 372-73. Furthermore, Location History logs a device’s location as  
14 often as every two minutes – regardless of whether any app is open or closed, the phone is in use,  
15 or the device is in a public or private space. *Id.* at 20, 114-15, 436–37, 513.

16           By contrast, the precision of CSLI “depends on the geographic area covered by the cell site.”  
17 *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person “within a wedge-shaped  
18 sector ranging from one-eighth to four square miles,” for example. *Id.* at 2218. As a result, a  
19 single CSLI data point could be used to determine which neighborhood or zip code someone was  
20 in, but it would not be accurate enough to identify the block and building. Moreover, even  
21 though cell phones ‘ping’ nearby cell sites several times a minute, service providers only log  
22 when the phone makes a connection, by placing a phone call or receiving a text message, for  
23 example. *Id.* at 2211.

24           These differences between Location History and CSLI are significant because they affect  
25 how much data is needed to infer where someone was and what they were doing. While  
26 *Carpenter* anticipated that the precision of CSLI would improve, 138 S. Ct. at 2218-2219, the  
27 Court was also faced with the fact that it was still necessary to stitch together some minimum  
28 amount of CSLI to reveal the “privacies of life.” The Court settled on seven days, but this was  
not a magic number; it was simply the number of days in the record for the shortest court order at

1 issue. *See* 138 S. Ct. at 2266-67 (Gorsuch, J., dissenting). And in fact, that order only produced  
2 two days of CSLI. *Id.* at 2212. As the State recognizes, *Carpenter* explicitly declined to say  
3 “whether there is any sufficiently limited period of time for which the Government may obtain  
4 an individual's historical CSLI free from Fourth Amendment scrutiny.” *Id.* at 2217 n.3. But  
5 short-term searches may still be capable of revealing the “privacies of life,” *id.* at 2214, which  
6 was the Court’s main concern in both *Carpenter* and *Jones*.

7 Although *Jones* and *Carpenter* involved so-called “long-term” searches, what primarily  
8 motivated the Court in each instance was the risk of exposing information “the indisputably  
9 private nature of which takes little imagination to conjure: ‘the psychiatrist, the plastic surgeon,  
10 the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the  
11 by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and  
12 on.’” *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d  
13 433, 441–42 (2009)); accord *Carpenter*, 138 S. Ct. at 2215. Thus, “[i]n cases involving even  
14 short-term monitoring, some unique attributes of GPS surveillance ... will require particular  
15 attention.” *Jones*, 565 U.S. at 415. The same is true for cell phone location information, given  
16 that “[a] cell phone faithfully follows its owner beyond public thoroughfares and into private  
17 residences, doctor’s offices, political headquarters, and other potentially revealing locales.”  
18 *Carpenter*, 138 S. Ct. at 2218.

19 But even before *Jones* and *Carpenter*, the Supreme Court was concerned with short-term  
20 location tracking, especially when it reveals information about the interior of a constitutionally  
21 protected space, such as a home. In *Karo*, the Court found that using an electronic beeper to track  
22 an object inside a private residence was a search. 468 U.S. at 716. A search occurs at the moment  
23 the object “has been withdrawn from public view.” *Id.* at 717. Especially relevant here, the Court  
24 remarked that “[i]ndiscriminate monitoring of property that has been withdrawn from public  
25 view would present far too serious a threat to privacy interests in the home to escape entirely  
26 some sort of Fourth Amendment oversight.” *Id.* at 716. So too in *Kyllo*, the Court found that  
27 using a thermal imaging device to peer through the walls of a private residence was a search. 533  
28 U.S. at 37. It was a search despite the fact that the scan “took only a few minutes” and could not

1 show people or activity inside. *Id.* at 30. As the Court explained, “[t]he Fourth Amendment’s  
2 protection of the home has never been tied to measurement of the quality or quantity of  
3 information obtained.” *Id.* at 37.

4 Location History’s greater precision and frequency of collection means that less time is  
5 needed to reveal the “privacies of life.” It might take days of CSLI to piece together a mosaic  
6 with enough detail to be so revealing, but it takes just a little Location History to achieve the  
7 same end. In this case, three hours and 40 minutes was more than sufficient to identify users in  
8 sensitive and constitutionally protected areas, including private residences in a dense residential  
9 neighborhood of San Francisco.<sup>3</sup>

10 Although Google initially “anonymized” this data, it is trivial to determine the likely  
11 identities of individuals inside their homes. *See* Def. Ex. D at 62–70; Hr’g Tr. at 83, 87–88, 90–  
12 91 Jan. 21, 2020, *United States v. Chatrie*, No. 3:19-cr-00130 (Def. Exhibit E). This is why  
13 Google treats Location History data not as a “business record” but as sensitive user “content”  
14 under the Stored Communications Act, 18 U.S.C. § 2703. This means that as far as Google is  
15 concerned, Location History is on par with the contents of an email or personal documents stored  
16 remotely on Google Drive. *See* Mot. to Quash & Suppress Evidence, Exhibit A at 9, 17 (“Google  
17 Amicus”). Far from an ordinary “business record,” Google considers Location History to be a  
18 “digital journal” of users’ movements and travels. *Id.* at 16. As a result, Google requires the  
19 government to obtain a warrant supported by probable cause to access Location History records.  
20 *Id.* at 15-18. There is no exception for four hours of data.

21 Furthermore, once the State seizes the “anonymized” Device IDs, it could simply obtain the  
22 subscriber information for any Device ID by issuing a subpoena to Google. *See Matter of Search*  
23 *of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 756 (N.D. Ill.  
24 2020) at 754 (“Fuentes Opinion”) (finding “no practical difference between a warrant that  
25 harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that

---

26 <sup>3</sup> It is important to note that the effective range of the Location History data seized in this case  
27 extended far beyond the boundaries of the geofence coordinates. This is due to the margin of  
28 error (“Display Radius”) that Google assigns to each Location History data point. The largest  
Display Radius in this case was 58 meters, which extends the effective range of the geofence  
warrant to cover dozens of private residences.

1 the government may easily use to learn the subscriber identities, and a warrant granting the  
2 government unbridled discretion to compel Google to disclose some or all of those identities.”).

3 The Supreme Court has repeatedly found precise, short-term searches to run afoul of the  
4 Fourth Amendment. See *Karo*, 468 U.S. at 716, and *Kyllo*, 533 U.S. at 37. And, based on these  
5 principles, other courts with occasion to consider a geofence warrant have recognized the private  
6 nature of Location History data. See *Matter of Search of Information Stored at Premises*  
7 *Controlled by Google*, 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) at 737 (“Fuentes Opinion”)  
8 (“[T]here is much to suggest that *Carpenter*’s holding, on the question of whether the privacy  
9 interests in CSLI over at least seven days, should be extended to the use of geofences involving  
10 intrusions of much shorter duration.”); *Matter of Search of Information Stored at Premises*  
11 *Controlled by Google*, No. 20 M 297, 2020 WL 5491763, at \*5 n7 (N.D. Ill. July 8, 2020)  
12 (“Weisman Opinion”) (“The government’s inclusion of a large apartment complex in one of its  
13 geofences raises additional concerns ... that it may obtain location information as to an  
14 individual who may be in the privacy of their own residence”).

15 Indeed, as Justice Gorsuch asked in *Carpenter*, “[W]hat distinguishes historical data from  
16 real-time data, or seven days of a single person’s data from a download of *everyone*’s data over  
17 some indefinite period of time? ... On what possible basis could such mass data collection  
18 survive the Court’s test while collecting a single person’s data does not?” 138 S. Ct. at 2267  
19 (Gorsuch, J., dissenting) (emphasis in original). The State struggles to argue that Location  
20 History is different, but Justice Gorsuch is correct. There are no principled distinctions to be had.  
21 Mr. Dawes had a reasonable expectation of privacy in his Location History data based on the  
22 Supreme Court’s decisions in *Carpenter*, *Jones*, *Karo*, and *Kyllo*.

23 **B. The Third-Party Doctrine Does Not Apply.**

24 The State contends that the “third-party doctrine” forecloses any expectation of privacy in  
25 Location History data, Opp. at 7, but the Supreme Court has never sanctioned a warrantless  
26 search of an individual’s cell phone location data, let alone the search of millions at once. See  
27 138 S. Ct. at 2219 (noting that the Court has “shown special solicitude for location information  
28 in the third-party context”). Indeed, the *Carpenter* Court declined to extend the third-party



1 doctrine to similar data and instructed lower courts not to “mechanically” apply old rules to new  
2 technologies. *Id.* Yet that is precisely what the government asks this Court to do: mechanically  
3 apply precedent from the 1960s and 70s to the technology of 2021.

4 The government invites error by likening Location History to the “invited informant” in  
5 *Hoffa v. United States*, 385 U.S. 293, 302 (1966)), as if Google were no different from the guy  
6 who Jimmy Hoffa conspired with in his hotel room. Opp. at 7. The *Hoffa* Court found it  
7 dispositive that the informant was not only in the suite by invitation, but that “every conversation  
8 which he heard was either directed to him or knowingly carried on in his presence.” *Hoffa*, 385  
9 U.S. at 302. Location History, by contrast, runs imperceptibly in the background, constantly  
10 recording, even if a user is doing nothing on the device. As with CSLI, “[v]irtually any activity  
11 on the phone”—or no activity at all—generates Location History data, even if the user is asleep.  
12 *See* Def. Ex. D at 122 (“[T]here were no periods of data not being collected.”).

13 The government also heavily relies on *Smith v. Maryland*, 442 U.S. 735 (1979). There, the  
14 Court found no expectation of privacy in the digits dialed from a landline telephone. 442 U.S. at  
15 742. The Court found it highly significant that callers were actively aware that they were  
16 interacting with the phone company when they placed a call, sometimes speaking with an  
17 operator, and receiving monthly bills with printouts showing the information collected. *Id.* at  
18 742-45. In this case, by contrast, Location History was likely enabled without Mr. Dawes even  
19 realizing it—meaning he would have had no awareness that it was on, silently recording, every  
20 two minutes. He would not have known Location History was enabled, let alone how much data  
21 was being collected or how to manage it. There is no evidence that Google sent reminders to Mr.  
22 Dawes. And Google does not bill users for Location History, unlike the digits dialed in *Smith*.  
23 *See* Google Amicus at 22. Consequently, Location History is not a “business record;” it is user  
24 data—content—that belongs to the individuals who created it. *See id.* at 8.

25 The State’s reliance on *United States v. Miller*, 425 U.S. 435 (1976), is likewise misplaced.  
26 In *Miller*, the Court found no expectation of privacy in checks, deposit slips, and statements  
27 because they were “*negotiable instruments*” intended for use in commercial transactions. 425  
28 U.S. at 438 (emphasis added). The Court distinguished them from otherwise “confidential

1 communications.” *Id.* Location History data, by contrast, is considered “content” under the  
2 Stored Communications Act, *see* 18 U.S.C. § 2703(a) & (b), and Google treats it accordingly.  
3 *See* Google Amicus at 4. And in any event, Location History data is not a “negotiable  
4 instrument.” No one gets paid in Location History. Rather, Location History is private data  
5 belonging to individual users that Google does not provide to advertisers. *See* Def. Ex. D at 197  
6 (regardless of the type of advertising, Google “never share[s] anyone’s location history with a  
7 third party.”); *see also* *Carpenter*, 138 S. Ct. at 2212 (wireless carriers “often sell aggregated  
8 location records to data brokers, without individual identifying information”).

9 In sum, Location History is not an “invited informant.” It is not a “business record.” And it is  
10 not a “negotiable instrument.” It is, however, significantly more revealing than the bank records  
11 in *Miller* or the telephone numbers in *Smith*. *See* *Carpenter*, 138 S. Ct. at 2217 (“After all, when  
12 *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever  
13 its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and  
14 comprehensive record of the person’s movements.”). Rather, Location History data is most like  
15 the cell site location information (“CSLI”) at issue in *Carpenter*, in which the Supreme Court  
16 found the third-party doctrine inapplicable.

### 17 **C. California Law Recognizes an Expectation of Privacy on Location History Data**

18 The State wholly fails to address the California Electronic Communications Privacy Act  
19 (CalECPA) when discussing whether Mr. Dawes had a reasonable expectation of privacy in his  
20 location history data. Instead, it only relies on an analysis of Fourth Amendment federal law.  
21 This is a gross oversight. The mere existence of the CalECPA is evidence of a reasonable  
22 expectation of privacy, in fact, it is evidence of a *recognized* expectation of privacy in the exact  
type of electronic data sought in this case.

23 Using the United States Supreme Court’s powerful and carefully defined limits on police  
24 searches of cell phones in *Riley v. California*, 573 U.S. 373 (2014), in 2016 the California  
25 legislature explicitly expanded privacy protections under CalECPA and codified these  
26 expectations of privacy for Californians. The legislative history of CalECPA clearly  
27 demonstrates that lawmakers were concerned with “properly safeguard[ing] the robust  
28 constitutional privacy...rights of Californians.” Sen. Comm. On Pub. Safety, Rep. on Sen. Bill  
178 (2015-2016 Reg. Session) March 24, 2015, p.11. Specifically, the legislature was interested

1 in updating existing “...California statutory law for the digital age.” *Id.* In discussing the need  
2 for the statute, one of the two authoring State Senators, Mark Leno, explained that “[f]or too  
3 long, California’s digital privacy laws have been stuck in the Dark Ages...[t]hat ends today with  
4 Governor’s signature of CalECPA, a carefully crafted law that protects personal information of  
5 all Californians.” Zetter, Kim. *California Now Has the Nation’s Best Digital Privacy Law*, Wired  
6 Magazine, Oct. 10, 2015, <https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/> (Last accessed September 12, 2021).

7 The edicts of CalECPA must be complied with in every “warrant for electronic information,”  
8 Pen. Code § 1546.1(d), and apply to every attempt by the government to “access electronic  
9 information by means of physical interaction or electronic communication with the electrical  
10 device.” Pen. Code § 1546.1(a)(3). This statute embodies California’s commitment to  
11 safeguarding the digital information of its residents—and clearly here. The location history data  
12 of Mr. Dawes falls squarely within these parameters. Indeed, it seems apparent that, contrary to  
13 the position it is taking now, the government has *already* acknowledged that Mr. Dawes had a  
14 reasonable expectation of privacy in this data, because they already sought a warrant for this data  
15 (albeit one that is defective under both the Fourth Amendment and CalECPA).<sup>4</sup>

16 The statutorily recognized expectation of privacy in this data is also evidenced in the ways in  
17 which CalECPA actually extended privacy protections beyond the Fourth Amendment.  
18 CalECPA specifies four additional areas with which a warrant “**shall** comply” when it comes to  
19 particularity in requests for electronic data: 1) the time periods covered by the warrant; 2) the  
20 target individuals or accounts; 3) the “apps” or services covered; and 4) the “types of  
21 information” sought. Pen. Code § 1546.1(d)(1). This language is explicitly tailored to digital  
22 information, it demands particularity to a greater degree than both federal law and the Fourth  
23 Amendment case law, and it reflects the legislative intent to update California law for the digital  
24 age. Indeed, CalECPA goes on to add additional regulations related to the specific retention,  
25 sealing, and disclosure of digital information. Pen. Code § 1546.1, as amended by Stats. 2016,  
26 ch. 541 (S.B. 1121) § 3.5. These provisions are clear evidence of the intent to protect  
27 Californians’ digital information. This language is not, as the prosecution implies, mere window

28 <sup>4</sup> Dawes is not addressing these warrant deficiencies in this briefing—this briefing only pertains to the limited and bifurcated issues of reasonable expectation of privacy. Dawes reserves the right to argue deficiencies of the warrant in future briefing.

1 dressing. In fact, the 2010 *People v Robinson*, 47 Cal. 4<sup>th</sup> 1104 (2010), case cited by the  
2 prosecution to argue that CalECPA does not demand greater particularity not only pre-dates the  
3 enactment of 2016’s CalECPA, so obviously does not address it, but also only discusses  
4 particularity in the Fourth Amendment context. Opp. at 11. Nothing the prosecution has cited  
5 supports their argument that CalECPA is less protective than the Fourth Amendment, and in fact,  
6 CalECPA stands “head and shoulders above federal law in protecting the privacy of modern  
7 communications” because it requires warrants for more investigations, the warrants impose more  
8 restrictive requirements, it provides notice to target individuals and accounts, and it expressly  
9 permits suppression of unlawfully obtained data. Susan Friewald, At the Privacy Vanguard:  
10 California’s Electronic Communications Privacy Act (CalECPA), 33 Berk. Tech. Law J. 131  
11 (2018).

12 Furthermore, CalECPA’s explicit suppression remedy is also strong evidence that  
13 Californians have a reasonable expectation of privacy in this data. The State misunderstands how  
14 CalECPA interacts with article 1 section 28 of the California Constitution *See* Opp. at 11.  
15 Exclusion for a violation of CalECPA itself is expressly permitted. After 1984 and the Right to  
16 Truth in Evidence Initiative, it is true that a California judge could not grant a suppression  
17 remedy based on the California Constitution or state law alone, *unless* the underlying statute was  
18 passed by at least two-thirds majority and the statute expressly permitted suppression. Cal.  
19 Const. art 1 § 28(f)(2). Because CalECPA passed by a two-thirds majority through each house of  
20 the California State legislature,<sup>5</sup> the remedies of suppression and exclusion of “any tangible or  
21 intangible thing obtained as a result of search or seizure” are absolutely available under  
22 CalECPA. Pen. Code § 1546.4(a); *cf. People v. Jackson*, 129 Cal.App.4th 129, 153 (2005)  
23 (suppression of evidence under state wiretap statute not prohibited by truth in evidence clause);  
24 Cal. Const. art 1 § 28(f)(2).

25 Therefore, even if the Fourth Amendment decisional law was not prevailing on the question  
26 of whether Mr. Dawes had a reasonable expectation of privacy, CalECPA demands that the  
27 Court “suppress evidence obtained or retained in violation of the Fourth Amendment to the  
28

---

<sup>5</sup> S.B. 178 passed the Senate by a vote of 34 to 4, with 2 abstentions, and passed the Assembly by a vote of 57 to 13 with 10 abstentions. S.B. 178 Privacy: Electronic Communications: Search Warrant (2015–2016), CAL. LEGISLATIVE INFO., [https://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill\\_id=201520160SB178](https://leginfo.legislature.ca.gov/faces/billVotesClient.xhtml?bill_id=201520160SB178) [<https://perma.cc/5GRD-SH4R>]

1 United States Constitution *or of this chapter.*” Pen. Code § 1546.4(a); *See also* Legislative  
2 Counsel’s Digest (2), 2015 Cal. Legis. Serv. Ch. 651 (S.B. 178). The suppression remedy is  
3 listed in the disjunctive, meaning a violation of *either* the Fourth Amendment *or* CalECPA  
4 warrants suppression. Suppression is therefore available as a remedy for a statutory violation,  
5 even if suppression is not required under the Fourth Amendment. *See* Pen. Code § 1546.4(a);  
6 Caskey, Cal. Search & Seizure (April 2018) 18 § 10:1. Overall, because CalECPA provides  
7 greater privacy protection specifically for the type of location history data sought here and  
8 because this statute provides a distinct remedy for suppression, there is clear evidence of a  
reasonable expectation of privacy in this data.

9 **2. Mr. Dawes Did Not “Voluntarily” Convey His Location History Data to Google.**

10 The State contends that Mr. Dawes did not have an expectation of privacy in his Location  
11 History data because he “made no efforts to shield it from law enforcement” and “expressly  
12 agreed” to a 2018 Google “Privacy Agreement.” [State at 6-7]. But as a factual matter, there is  
13 no evidence that Mr. Dawes did any such thing. Rather, an expert examination of Google logs  
14 for Mr. Dawes’ account shows that Location History was enabled, likely by default, when Mr.  
15 Dawes set up a new cell phone and created his Google account in 2015. *See* Def. Ex. B at 6.  
16 Consequently, Mr. Dawes was unaware that Google was collecting his Location History data and  
17 he would not have known to turn it off or delete it.

18 Google provided Mr. Dawes with an “audit log” for his account, in partial satisfaction of the  
19 subpoena still outstanding in this case. *See* Google Account Change History at 2 (Mar. 2, 2021)  
20 (Def. Exhibit F). According to an expert retained by Mr. Dawes, Spencer McInville, that log  
21 shows the details of the creation of Mr. Dawes’ Google account. Def. Ex. B at 3. It shows that  
22 Mr. Dawes created his account on March 9, 2015, during the initial setup of a new cell phone,  
23 and that within 11 seconds, Location History had been enabled. *Id.*

24 Google has not provided specific information about how that process occurred, or what  
25 language, if any, Mr. Dawes would have seen on his phone at the time with respect to Location  
26  
27  
28

1 History.<sup>6</sup> However, Mr. McInville was able to recreate the 2015 setup process on a test device  
2 and recorded video and screenshots of it. *See* Def. Ex. B at 4-5; Def. Ex. C. It never mentions  
3 Location History once. Furthermore, there is only one screen that concerns location information  
4 at all, and Google has confirmed that none of the checkbox options concern Location History.  
5 Def. Ex. B at 5. Consequently, Mr. McInville concluded that Location History was enabled  
6 “automatically” at the initial setup “with no user consent requests.” *Id.* at 6. In short, Mr. Dawes  
7 was given no choice and no notice that his Location History was being collected.

8 The government points out that it was possible to disable Location History and delete saved  
9 records in 2018. *Opp.* at 8. But this assumes that Mr. Dawes was both fully aware of the  
10 collection taking place as well as knowledgeable about how to control or stop it, and the  
11 government has offered no evidence to indicate that this was the case. On the contrary, it would  
12 have been counterintuitive and difficult for Mr. Dawes to disable and delete, assuming he even  
13 knew about its existence. Deleting Location History data does not turn off Location History. *Def.*  
14 *Ex. D* at 361. And once enabled, Location History can never be turned “off,” only “paused.” *See*  
15 *Def. Ex. D* at 360-61. Furthermore, it is only possible to “pause” Location History by navigating  
16 through complicated settings menus and disregarding a pop-up warning from Google that doing  
17 so will “limit[] functionality” on the device. *See id.* Similarly, while pressing “pause” means that  
18 no future data will be recorded, it does not delete any past data collected. *See Def. Ex. D* at 356,  
19 361. In this light, Location History is designed like a lobster trap: easy to get in, hard to get out.

20 **3. Even if Mr. Dawes Intentionally Enabled Location History, the Third-Party Doctrine**  
21 **Would Still Not Apply.**

22 Timothy Carpenter signed a contract with his cell phone service provider. *Carpenter*, 138 S.  
23 Ct. at 2225 (Kennedy, J., dissenting). He did not allege that he was tricked or coerced into it.  
24 And yet, the Supreme Court still found that he was not “voluntarily” conveying his location data  
25 to the service provider, even though everyone was aware that that is how cell phones work. *Id.* at

---

26  
27 <sup>6</sup> In fact, this is the information Mr. Dawes still seeks through subpoena to Google. Mr. Dawes  
28 believes it will show that he did not consent to enabling Location History and that any purported  
consent was not knowing, informed, or voluntary.

1 2220 (“Cell phone location information is not truly ‘shared’ as one normally understands the  
2 term.”). Indeed, the Supreme Court has never allowed such agreements to determine the contours  
3 of the Fourth Amendment. *See Smith*, 442 U.S. at 745 (“We are not inclined to make a crazy  
4 quilt of the Fourth Amendment”). And rather than “mechanically” applying the third-party  
5 doctrine, the *Carpenter* Court looked at the context—whether the “choice” to hand over the data  
6 truly outweighed the privacy intrusions given the realities of the digital age. *Id.* at 2219–20. The  
7 majority never once mentioned the contract or terms of service.

8 The Court’s contextual concern exists here in abundance. “[M]echanically” applying the  
9 third-party doctrine here would divest, at a minimum, tens of millions of people of their Fourth  
10 Amendment rights merely for participating in normal everyday life. *See* Def. Ex. D at 205.  
11 Google Location History may not be a pillar of digital society, but there are still “numerous tens  
12 of millions” of people who use it, wittingly or not. The *Carpenter* Court remarked on the  
13 pervasiveness of cell phones in the United States. 138 S. Ct. at 2220 (citing *Riley v. California*,  
14 134 S. Ct. 2473, 2484 (2013)). At issue here is one-third of all Google users. It would be  
15 nonsensical to deem this data unworthy of Fourth Amendment protection unless everyone is  
16 using it, yet that is the line the government seeks to draw.

17 Here, the State invites this Court to conclude, contrary to the facts, that Mr. Dawes intended  
18 to enable Location History and disclose a dossier of his every move to law enforcement based on  
19 a 2018 “Privacy Agreement.” *Opp.* at 6-7. But even if Mr. Dawes had done so, the existence of a  
20 privacy policy would not end the Fourth Amendment inquiry. On the contrary, the *Carpenter*  
21 Court looked beyond this question, considering context, common sense, and the sensitivity of the  
22 data, to hold that the sharing of cell phone location data was not truly “voluntary.”

23 In this case, the 2018 Google “Privacy Agreement” only mentions Location History twice.  
24 The first line casts Location History as a way to “save and manage location information in your  
25 account.” *Opp.* Ex. 3 at 4. The other line, in passing, states that “you can turn on Location  
26 History if you want traffic predictions for your daily commute.” *Id.* at 8. These brief mentions  
27 sow only further confusion and do not explain to users what Location History is, how it collects  
28

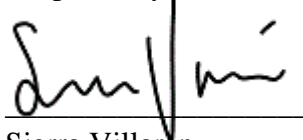
1 location information, or that it may already be on. And they certainly do not amount to  
2 meaningful or voluntary consent.

3 As Judge Fuentes determined in Illinois, it is “difficult to imagine that users of electronic  
4 devices would affirmatively realize, at the time they begin using the device, that they are  
5 providing their location information to Google in a way that will result in the government's  
6 ability to obtain – easily, quickly and cheaply – their precise geographical location at virtually  
7 any point in the history of their use of the device.” Fuentes Opinion, 481 F. Supp. 3d at 737. So  
8 too should this Court look to the realities of the digital age and recognize that the voluntary  
9 exposure rationale underlying the third-party doctrine does not hold up when it comes to  
10 Location History data.

11 **Conclusion**

12 For the foregoing reasons, Mr. Dawes asks this Court find that he had a reasonable  
13 expectation of privacy in his Location History data. In the alternative, Mr. Dawes requests that  
14 this Court fully enforce Mr. Dawes’ subpoena to Google seeking information about the process  
15 of enabling Location History in 2015.

16  
17 Respectfully submitted,

18 

19  
20 Sierra Villaran  
Deputy Public Defender

21  
22 Michael Price  
NACDL  
23 Counsel for LaQuan Dawes  
24  
25  
26  
27  
28



1 **Proof of Service**

2  
3 I say:

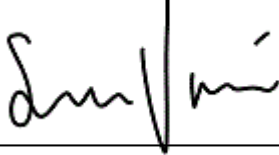
4 I am over eighteen and not a party to the above action. My business address is 555 Seventh  
5 Street, San Francisco, California 94103.

6 I caused to be served copies of the attached Reply to States Opposition to Motion to Quash,  
7 by transmitting via my electronic service address (sierra.villaran@sfgov.org), to the persons at  
8 the email addresses set forth below:

9 Bianca Calderon-Penaloza  
10 San Francisco District Attorney  
11 350 Rhode Island Street  
12 North Building, Suite 400N  
13 San Francisco, CA 94103

14 I declare under penalty of perjury that the foregoing is true and correct.

15 Executed on September 13, 2021 at San Francisco, California.

16   
17  
18 \_\_\_\_\_

19 Sierra Villaran  
20  
21  
22  
23  
24  
25  
26  
27  
28