ELECTRONIC FRONTIER FOUNDATION
SAIRA HUSSAIN (SBN 300326)
AARON MACKEY (SBN 286647)
F. MARIO TRUJILLO (SBN 352020)
ADAM SCHWARTZ (SBN 309491)
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Email: saira@eff.org
amackey@eff.org
mario@eff.org
adam@eff.org

VALLEJO | ANTOLIN | AGARWAL | KANTER LLP
MONTY AGARWAL (SBN 191568)
RACHEL CHANIN (SBN 229253)
3021 Citrus Circle, Suite 220
Walnut Creek, CA 94598
Telephone: (925) 951-6970
Email: magarwal@vaakllp.com
rchanin@vaakllp.com

Attorneys for Petitioners

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SACRAMENTO

ASIAN AMERICAN LIBERATION NETWORK, a California non-profit public benefit association; KHURSHID KHOJA, an individual; ALFONSO NGUYEN, an individual,

Petitioners/Plaintiffs,

v.

SACRAMENTO MUNICIPAL UTILITY DISTRICT; PAUL LAU, in his official capacity as the Chief Executive Officer of the Sacramento Municipal Utility District; CITY OF SACRAMENTO; KATHERINE LESTER, in her official capacity as Chief of Police of the City of Sacramento Police Department,

Respondents/Defendants.

Case No.: 34-2022-80004019

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PETITION FOR WRIT OF MANDATE

Hearing Date: October 10, 2025
Time: 10:00 a.m.
Place: Department 21
Judge: Hon. Shelleyanne W. L. Chang

Action Filed: September 21, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitution

INTRODUCTION

This case is about Sacramento Municipal Utility District's ("SMUD") and law enforcement's dragnet surveillance of SMUD customers' homes using sensitive and confidential energy usage information. The decade-long surveillance violates the California Constitution and a state privacy statute.

Between 2009 and 2014, SMUD rolled out advanced metering infrastructure, including wirelessly connected "smart meters" installed for 99.9% of its customers. Unlike their analog predecessors, smart meters scoop up energy usage data continuously, in 15-minute increments, and transmit this data to SMUD wirelessly every few hours. SMUD uses the "interval data" from the smart meters to discern what might be happening inside its customers' homes. This interval data can reveal a wealth of private information, including when customers are sleeping or awake or demographic information such as employment status or family size. SMUD analysts can, in effect, use the data to digitally peer into a person's home.

SMUD uses sophisticated software to analyze smart meter data. The software's initial purpose was to help SMUD find power theft. But for the last decade, SMUD analysts have actively collaborated with law enforcement—and especially the Sacramento Police Department—by providing lists, opinions, and tips in a hunt for SMUD customers who might be growing cannabis. Specifically, law enforcement sends requests for, and SMUD discloses, lists of all customers in a given zip code that use above a minimum threshold of electricity. Often, these requests span the zip codes for an entire city. One such list included more than 10,000 customers. SMUD analysts then scrutinize the smart meter interval data, going "account by account" in a "painstaking" process, and opine if a customer is a "pattern" user, or speculate about the number of lights a customer might be using to grow cannabis. The Sacramento Police Department requests this data quarterly.

The data sharing has no apparent rules. Most often, SMUD provides customer data based on a form that SMUD disseminates and pre-prints with the words "ongoing

investigation" — a conclusory recitation of words from a controlling statute. But neither SMUD nor law enforcement has any criteria for complying with this legal standard, or with any other. Sometimes SMUD analysts will affirmatively send a text message to an officer after studying interval data to invite police inquiry: "Send me a request for [two particular addresses]. One is 10k plus, and the other is 4k, Asian…." SMUD analysts even look at credit databases and offer observations like, "interesting thing about the [] address is the multiple Asians that have reported there…."

SMUD's lists, opinions, and tips are often wrong, and law enforcement frequently uses the information in abusive ways. Customers have reported feeling "criminalized" and "highly upset" at law enforcement showing up at their homes or sending what a SMUD analyst called "nastygrams" accusing them of growing cannabis. Law enforcement has appeared at customers' homes based on SMUD's tips, only to find nothing more than a large fish tank, a man cave, or a large house. Sacramento County Sheriff's Office deputies went to one Petitioner's home "per SMUD." When Petitioner stated that he was not growing cannabis and refused a search, a deputy called him a liar. A medical condition explained his electricity usage. Another SMUD customer had to walk out in his underwear to guns and sirens, with neighbors onlooking, because SMUD told law enforcement that he was growing cannabis based on a "7pm to 7am" usage pattern. He was mining cryptocurrency.

This data sharing and surveillance is illegal. Article I, § 13 of the California Constitution prohibits unreasonable searches. SMUD and law enforcement's home energy surveillance program is an unreasonable search. The conduct also violates Public Utilities Code § 8381, a privacy statute that bars public utilities from disclosing customers' electrical consumption information except in narrow circumstances.

Petitioners are taxpayers who have a beneficial interest and public interest in stopping SMUD and law enforcement's illegal surveillance program. They ask this Court to command SMUD and the City of Sacramento, whose Sacramento Police Department is one of the most prolific users of SMUD data, to comply with the law.

STATEMENT OF FACTS

1. SMUD collects customer smart meter interval data.

SMUD is a community-owned electric service provider formed under California's Municipal Utilities District Act. (Petitioners' Record Evidence in Support of Petition for Writ of Mandate ("Record") at 814, 555.) It has about 650,000 customers, mostly in Sacramento County. (Record 241, 555.) Customers have no alternative to SMUD, the only electricity provider in its region. (Record 1316, 555.)

Between 2009 and 2014, SMUD built out an advanced metering system. SMUD transitioned customers from analog meters to "smart meters" by default. SMUD incentivizes smart meter adoption by adding opt-out fees: a one-time fee of $145 and a monthly fee of $14. (Record 559, 572–574, 718.) Some customers in multi-family homes or apartments cannot opt out. (Record 572–574, 718.) SMUD has installed smart meters for 99.9% of its customers. (Record 244–245.)

Smart meters give SMUD exponentially more consumption data than their analog predecessors. (Record 809.) Whereas analog meters convey the prior month's total without further granularity, SMUD's smart meters collect usage information in 15-minute increments. (Record 815, 1908.) They send that data to SMUD multiple times daily via a wireless network. (Record 584, 586, 718, 738.)

SMUD keeps this data for years. (Record 669–670, 675, 718.) SMUD's analysts can look at an individual customer's usage patterns during specific days, weeks, or months as far back as eight years. (Record 1262:8–1263:24, 1269–1271.)

2. SMUD customers' smart meter data is private.

SMUD's customers have a strong privacy interest in their smart meter data because it exposes intimate details about domestic life.

SMUD's Policies. SMUD recognizes the sensitivity of its smart meter data. A SMUD internal policy declares that "Sensitive and Confidential Information" includes "all information gathered about our customers," such as "electricity usage." (Record 704, 718.) SMUD's Board of Directors also sets guidance, which states: "SMUD will

protect customer [] information" and "[e]xcept as provided by law or for a business purpose, SMUD will not disseminate sensitive and confidential customer information to a third party for non-SMUD business purposes unless the customer first consents to the release of the information." (Record 556, 736, 495–496, 718–719.) The Board policy is also referenced in its "Privacy Policy," linked at the bottom of SMUD's website. There, SMUD promises to "strictly enforce privacy safeguards." (Record 711–714, 719.)

Petitioners' Expert. Dr. Stephen Wicker is an emeritus professor at Cornell University who has conducted extensive research into smart meters. (Record 156, 159.) Smart meter data, he explains, "can be used to gain insights and draw conclusions about customers' personally identifiable information." (*Id.* at 162.) This includes data analyzed in one-hour increments. (*Id.* at 164, 169–170.) For example, "sudden increases in energy usage are likely indicative of customers being active within their homes performing actions such as activating indoor heating and cooling systems, cooking, or using lights," whereas decreases indicate "the customer going to sleep for the night or leaving their home." (*Id.* at 166.) With smart meter data, "showering can also be inferred, as electric water heaters used to heat shower water consume significant amounts of power." (*Id.* at 168.) Smart meter data also allows "inferences on customer demographics," including employment status and family size, and even religion and income. (*Id.* at 170–172.)

3. SMUD turns over lists, opinions, and recommendations to police.

SMUD uses sophisticated software that allows its analysts to search, filter, and visualize customers' smart meter data. (Record 81, 638, 718, 1238:17–1239:6, 1269–1271.) Over the years, SMUD has used various software: Detectent, UtilityIQ by Itron, and Voltron, the latter of which is SMUD's latest in-house version. (*See generally* Record 1188–1189, 1206, 1210, 1230–1244.) The initial purpose of this software was to "identif[y] and prioritize[] probable theft cases." (Record 636, 718.)

SMUD gives its Revenue Protection group access to the software and customer

data, including smart meter interval data. (Record 815, 772–773.) SMUD analysts Robert Duggan, Michael Wolff, and Jason Burkhalter work or have worked in the group to find power theft. (Record 237, 249, 772–773, 1187, 1228–1229, 1314–1315.)

For over a decade, however, these SMUD analysts have been using the software and customer data to provide law enforcement with lists of customers and opinions about what people might be doing inside their homes. The apparent aim is to feed law enforcement tips about *possible* residential cannabis grows. They have disclosed lists by zip code of all customers using electricity above a particular threshold to several local law enforcement agencies: Sacramento Police Department, Sacramento County Sheriff's Office, Elk Grove Police Department, and Rancho Cordova Police Department. (Record 5–68.) Law enforcement has requested or SMUD has provided such a "zip code list" at least 90 documented times over 10 years. (*Id.*)

In these zip code lists, SMUD typically provides law enforcement with customer names, addresses, and usage. Analysts frequently add opinions based on their study of customers' detailed smart meter interval data. (Record 1320–1322, 1324.) Although the zip code lists are sometimes called "high user" lists, law enforcement has over time lowered the threshold — from 7,000 kilowatt-hours ("kWh") in 2014 (Record 1328–1329) to 2,800kWh in 2023 (Record 1138–1181, 138.)[1] SMUD analysts agree that using 2,800kWh is not in any way suspicious. One wrote in a transmittal email: "This [list] is scraping the bottom of the barrel." (Record 19.) Another testified that it means "nothing" that a customer uses 2,800kWh. (Record 1194.) A third testified: "I used 3500 [kWh] last month." (Record 1267; *accord* 847–853, 855.)

One SMUD analyst testified he has never refused a law enforcement request for a zip code list. (Record 1220, 1225.) The result is that, to date, SMUD has turned over to law enforcement the names, addresses, and electrical consumption information of

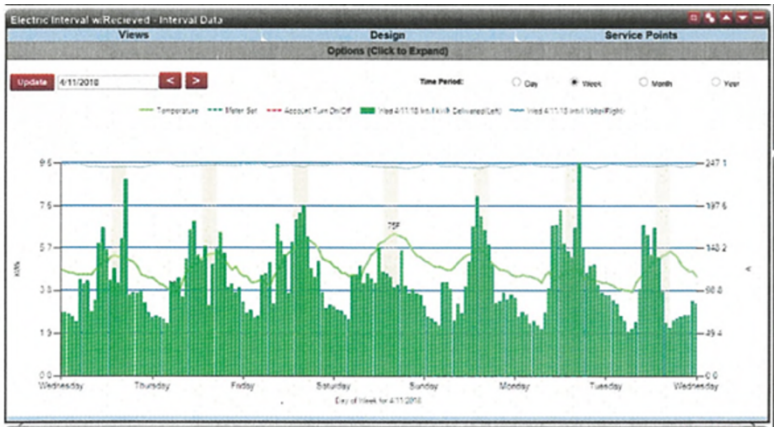
---

[1] A kilowatt-hour is a measure of electricity equal to one kilowatt of power expended for one hour. *Kilowatthour*, Glossary, U.S. Energy Information Administration, https://www.eia.gov/tools/glossary/index.php?id=K.

more than 33,000 customers through a zip code list. (Record 141.) Some customers' information appears on more than one zip code list. (*Id.*) The 33,000 customers make up about 5% of SMUD's total customer base of 650,000.[2]

SMUD analysts sometimes opine about what might be happening inside their customers' homes, including their views about the number of grow lights the analyst believes might be in use. (Record 8, 1320–1322.) SMUD analysts also have sent a list and then followed up with their opinions. (Record 1306, 1483, 1916, 1952.)

SMUD analysts reach their opinions by scrutinizing customers' detailed smart meter interval data. Below is an example of how a SMUD software system visualizes a customer's smart meter interval data for a week, with each bar representing an hour of usage. (Record 1245:6-10, 1269–1271, 1264–1265, 1190:17–1191:6.)



4. SMUD's sharing of customer data with Sacramento Police.

Officers at the Sacramento Police Department, in particular, have requested or SMUD has provided zip code lists more than 50 times over the past decade. (Record 6–68, 831, 842, 1217.) In recent years, the exchange has followed a predictable pattern. Typically, Lindsey Mendoza, a Sacramento Police analyst, sends to SMUD "Law Enforcement Customer Information Request" forms for every zip code in the City of

---

[2] This is likely an underestimate since SMUD could not produce many of its communications with law enforcement. (*See generally* Record 1461–1464.)

Sacramento roughly every quarter. (Record 1507–1553.) She asks, for instance, for a list of SMUD customers using "2,800kWh and above per month." (Record 1509.) Since this lawsuit's initiation and upon SMUD's advisement, she requests over 2,800kWh and "12-hr and/or 18-hr consumption patterns." (Record 1012–1014.)

SMUD analyst Burkhalter runs an initial search on all customer records for each zip code requested to capture those using above 2,800kWh in the last 30 days; he removes any commercial properties, and then sends the full list to Mendoza. (Record 1192–1193, 1195, 1222–1223, 1196–1198.) Mendoza then removes customers living outside the City and returns the filtered list to Burkhalter. (Record 832:3–833:10.)

Next, Burkhalter studies each customer's smart meter interval data (see chart above), going account by account, and opines whether the customer has "pattern" usage. (Record 1200, 1224.) Burkhalter described this as a "painstaking process" that takes "months" and is done on "separate time" that is "above and beyond" his "normal work scope." (Record 1200, 1202–1203, 1211, 1224.) Pattern usage looks "like columns," a spike followed by a flat pattern for a 12- or 18-hour block and then a dip, when the customer data is visualized via SMUD's software. (Record 1201–1202.)

The apparent theory is that pattern users *might* be indoor cannabis growers, although SMUD and Sacramento Police admit this is often not true. (*See infra* pp. 14–16.) (*See* Record 884 ("With the KWH floor [so] low, there could be multiple reasons for pattern usage, [like] electric heat, space heaters, etc."), 863 ("2,800 KWH and pattern usage will probably include a lot of accounts with electric heat"), 1488 (even with a "good grow pattern," police "have to be careful," given "this lower kWh range").) (*See also* 1204–1205 ("lots of air-conditioning in the summertime, big pools, but many different things" could "render a false positive").)

The process for SMUD sharing customer data in one recent quarter is illustrative. In July 2023, Mendoza sent requests for customers using "2,800kWh and above per month" for the 23 zip codes in the City of Sacramento. (Record 1507–1553.) Burkhalter responded with a 210-page list of over 10,000 customers' names, addresses,

and electrical usage data, followed by a shorter list from two overlooked zip codes. (Record 1555–1769.) After Mendoza removed non-City customers, there remained "4,800 locations left for [Burkhalter] to check patterns on." (Record 1771–1873.) Months after studying interval data, in October 2023, Burkhalter reported his opinion — four "lucky winners with pattern usage." (Record 1876.) He cautioned, "Make sure you guys do your own investigation because there's tons [of] a/c." (Record 1875.)

SMUD also proactively mines and discloses customer data to police, including:

- SMUD analyst Michael Wolff, acting on his own initiative, sent a text message to a Sacramento Police officer, saying, "Send me a request for [two particular addresses]. One is 10k plus, and the other is 4k, Asian and been there less than 3 months." (Record 1298; *see also* 1301–1302 (corresponding email/request form), 1304–1307 (response email).)
- Wolff observed, in response to a police email for a specific address, "One interesting thing about the [] address is the multiple Asians that have reported there through Experian in 2017." (Record 1309.)
- A SMUD analyst testified that he would disclose customer data via text to police "on the fly." (Record 1325.)

SMUD's analysts are not mere data responders. A police architect of the data mining collaboration considers SMUD part of the "team." (Record 1373:14-21.) SMUD has coached law enforcement on how to request zip code lists. (Record 1293 (Wolff instructing: "The 'other information requested' box can be used to free form specific requests, such as high user zip codes. Be specific though!").) Wolff even accused Scott Rodd, a reporter who in 2019 published a multi-part series on Capital Public Radio's website regarding abuses by the City of Sacramento in its cannabis enforcement, of trying to "shut down the flow of information to law enforcement from SMUD." (Record

1252:15–1253:1.)[3] Police depend on SMUD analysts' opinions drawn from studying customers' smart meter interval data. Mendoza said it would be "problematic" if SMUD did not provide these opinions because "that's some of the information we utilize to begin an investigation." (Record 844–846.)

5. Police only start investigating after getting SMUD's opinions.

Mendoza requests lists for virtually every zip code in the City (*see*, *e.g.*, Record 833, 1504, 1507-1553), and her previous supervisor, Sergeant Dustin Smith, testified that the investigation into illegal cannabis grows only starts *after* police obtain SMUD's zip code lists and opinions. (Record 1332, 844-46.) For instance, in 2023, a Sacramento Police officer obtained a warrant to search a home that originated from a SMUD zip code list. The supporting affidavit noted that he "initiated an investigation" only after getting information from SMUD. (Record 1355–1356; *see also* 1930.)

After Mendoza receives SMUD's list and opinions on pattern users, she correlates them with property information. (Record 832–836.) She notes on a spreadsheet information such as whether the owner is the same as the SMUD customer and any prior police contact. (Record 834–835.) Mendoza then gives the spreadsheet to police officers. For years, Mendoza sent her list to the officers with the customer names shown. (Record 838–839.) In 2019, the City of Sacramento was sued for, among other things, targeting the Asian community in connection with cannabis enforcement based on SMUD leads. *Wang v. City of Sacramento*, Case No. 34-2019-00264523 (Sac. Sup. Ct.). After the suit's resolution, Mendoza started redacting customer names from the list she sent to officers. (Record 836–837.)

For some customers who appear on the pattern-user list, Mendoza sends a letter to the owner and occupant. One SMUD analyst referred to these letters as

---

[3] *See* Scott Rodd, *When Tenants Grow Pot, Sacramento Homeowners Face Six-Figure Fines And An Appeals Process Attorneys Call 'A Kangaroo Court'*, Capital Public Radio (Sept. 26, 2019), https://www.capradio.org/articles/2019/09/26/when-tenants-grow-pot-sacramento-homeowners-face-six-figure-fines-and-an-appeals-process-attorneys-call-a-kangaroo-court/.

"nastygrams." (Record 1274.) The letters all but accuse the owner/occupant of growing cannabis and demand they contact the police. (Record 840–841, 1183–1184, *accord* 1333.) Prior to the *Wang* litigation, Mendoza sent these letters in English and Chinese, but no other language. (Record 856–861.)

Sometimes after getting Mendoza's pattern-usage list, officers "initiate" typical police investigatory steps: a drive-by, license plate checks, photos of the house, prior criminal history checks, and/or checking prior contact datasets. (*See*, *e.g.*, Record 1355–1358.) Police then sometimes seek search warrants. (Record 1332–1333.)

6. SMUD's lists, opinions, and tips ensnare innocent people.

In some supporting affidavits for search warrants, Sacramento Police officers declare that SMUD analysts have "never incorrectly assessed" electrical consumption data. (Record 1472, 1356). The evidence disproves this.

Behind the scenes, SMUD analysts caution police that many listed customers have "high" energy usage for innocent reasons (Record 1274, 1875, 1882). The low usage threshold captures, in SMUD's own words, "Christmas lights" (Record 894), "electric heat" (Record 970), "a/c" (Record 1875), and "big houses" (Record 875).

At deposition, SMUD analysts agreed that higher than average usage could be the result of air conditioning, a pool pump, an electric vehicle, electric heat, or a big house. (Record 1250–1251, 1194–1195, 1323–1324.) Sacramento Police employees testified similarly: High energy usage could include a large home, electric heat, air conditioning, Christmas lights, a heated swimming pool, cryptocurrency mining, growing vegetables in a hoop tent, three kitchen islands and an elevator, a man cave, a large fish tank, exotic plants, and a tiny home compound. (Record 847–853, 855, 1339–1341, 1344.) One Sacramento Police officer, reflecting on the inefficiency of SMUD's opinions, testified, "maybe I could have just drive[n] around East Sacramento and rolled down my windows and tried to smell something." (Record 1343.)

SMUD analysts often warn that even after screening homes for pattern usage, those on the list might not be growing cannabis. (*See* Record 884 ("With the KWH floor

[so] low, there could be multiple reasons for pattern usage"), 863 ("2,800 KWH and pattern usage will probably include a lot of accounts with electric heat"), 1488 (even with a "good grow pattern," police "have to be careful," given "this lower kWh range").)

SMUD has no policies capping how much electricity a customer can use. As SMUD analyst Wolff explained, "SMUD likes it when you use a lot of power." (Record 1266.) Accordingly, when SMUD discloses data and its analysts offer opinions, SMUD is not determining that any customer is violating any usage policy of SMUD. (Record 1215–1216, 1248–1249.) One analyst testified that his opinions are "[n]ot at all" a determination that a resident is illegally growing marijuana. (Record 1212–1213.)

Law enforcement has turned up at innocent people's homes based on SMUD's tips, resulting in residents feeling "criminalized" and "highly upset" at the privacy invasion. (Record 1345, 1342, 143–144; *see also* 1334 (sergeant agreed "[s]ome people were pissed off that they were being accused of committing a crime when they were not doing anything wrong").)

In May 2020, two Sacramento Sheriff's deputies showed up unannounced at the home of Petitioner Alfonso Nguyen. (Record 143, ¶ 3.) They demanded entry to conduct a search, accused him of growing marijuana, and said SMUD had reported that he used a lot of electricity. (*Ibid*.) They were there because SMUD reported his home's electrical usage to the Sheriff's office. (Record 146.) When Nguyen denied growing marijuana, and refused a search, a deputy called him a liar. (Record 143 ¶ 4.) Nguyen has never grown marijuana, and neither has anyone he lives with. (*Id*. at ¶ 1.) Rather, he consumes more than average electricity due to a spinal injury. He uses an electric wheelchair and must maintain his body temperature with the steady use of electric heat pumps and air conditioning. (*Id*. at ¶ 2.) As a result of the encounter, Nguyen feared for his physical safety and felt that his privacy had been invaded. (*Id*. at ¶ 7.)

Similarly, in 2020, at about 7:00 am, Sacramento Sheriff's deputies showed up at declarant Brian Decker's home with a warrant. (Record 221–222 ¶¶ 2, 4.) They were there because his name and home appeared on a SMUD list, and because SMUD told

law enforcement that "4 to 5 grow lights are being used [at his home] from 7pm to 7am." (Record 1952, 222 at ¶ 6.) With guns drawn and sirens and bullhorns blaring, they demanded that Decker come outside. (Record 221 ¶ 2.) Frightened, and with neighbors video recording the event, Decker was forced to walk backward out of his home in only his underwear. (*Ibid.*) When deputies found no cannabis growing operation, they asked why he was using so much power. (222–223 ¶ 5.) He was mining cryptocurrency. (*Ibid.*) Indeed, the surveillance program has led law enforcement to multiple homes mining cryptocurrency. (*See, e.g.*, Record 851–852, 1214.)

In another instance, Sacramento Police executed a warrant at a home that was growing residential cannabis within the lawful limit. (Record 1481, 1483–1486.) They have also returned warrants to the court noting that, "Officers did not locate any evidence of cultivation of Marijuana during the search." (Record 1367.) Nor did they find cannabis grows at many of the homes they inspected as a result of SMUD's pattern-usage list. (*See* Record 1345, 1342, 143–144.)

7. SMUD and law enforcement conceal their collaboration.

SMUD and law enforcement have tried to conceal the depth of their collaboration in the home energy surveillance program.

- In a 2018 email to Sacramento Police officer Kelli Streich, SMUD analyst Wolff said he "just would not want" screenshots of customer information that he was sharing, "showing up in the 'Sac. News & Review.'" (Record 1375.)
- In 2022, after media attention about this matter and customer complaints to SMUD, SMUD analyst Burkhalter demanded of Sacramento Police employee Mendoza, "when talking to the customer, leave SMUD out of it," even though SMUD has been deeply part of this surveillance program for over a decade. (Record 863, 1220–1221.)

8. Customers do not consent to SMUD's surveillance.

SMUD does not get, and customers have not given, consent to being surveilled and their information being disclosed. (Record 1251, 1326, 223.) SMUD has cited its

Privacy Policy as constituting blanket consent by all of its 650,000 customers to the surveillance. (Record 789.) Yet there is no mechanism by which a customer can give or refuse consent within the Privacy Policy or upon signing up for service—it is a non-conspicuous link at the bottom of SMUD's website. (*See* Record 1406–1409.) Furthermore, about 40% of SMUD's customers have a move-in date before SMUD adopted its bottom-of-page-linked Privacy Policy in August 2015. (Record 803.)

9. Neither SMUD nor law enforcement confirms that requests for customer information are made as part of an ongoing investigation.

To facilitate the SMUD and law enforcement surveillance program, Respondents use a pre-printed SMUD form, titled "Law Enforcement Customer Information Request." (*See*, *e.g.*, Record 1497–1498.) Although SMUD has revised the form over the years, a constant is that the top says the request is "part of an ongoing investigation" and cites to Government Code Section 6254.16(c) (now Section 7927.410(c)). After the filing of this lawsuit, SMUD added language to the form stating that the law enforcement officer "certifies" that the request is part of an ongoing investigation. (*Compare* Record 1501–1502 *with* 1497–1498.)

Sacramento Police analyst Mendoza, however, could not identify even one criterion she uses to determine or "certify" if a request is part of an "ongoing investigation," though she has been requesting customer information and SMUD's opinions for six years. (Record 842–843, 854.) SMUD analysts Burkhalter and Wolff likewise could not identify any criteria. (Record 1218–1219, 1254–1257.) Burkhalter could not think of any instance in which he refused a law enforcement request for customer information. (Record 1220, 1225.) Wolff said he always turned over his lists, opinions, and tips because law enforcement requests are "official." (Record 1246–1247.)

ARGUMENT

I. Respondents' energy surveillance violates the state Constitution.

Article I, § 13 of the California Constitution bars unreasonable searches.

Respondent's dragnet home energy surveillance program is a search, given its severe intrusion on SMUD customers' reasonable expectation of privacy in the data that SMUD collects about the interior of their homes. SMUD's searches with and for law enforcement are suspicionless and, therefore, *per se* unreasonable.

A. Article I, § 13 is more protective than the U.S. Constitution.

Article I, § 13 provides:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized.

Although Article I, § 13 is similar to the U.S. Constitution's Fourth Amendment and the two provisions "ordinarily" are construed "in tandem," California courts will rule "solely" under the former where, as here, the U.S. Supreme Court has not yet reached the issue. (*People v. Buza* (2018) 4 Cal.5th 658, 686).

Article I, § 13 is more protective, especially of the home. The California Supreme Court, for instance, held that people have a reasonable expectation of privacy against police aerial surveillance of their backyards. The U.S. Supreme Court held the opposite. (*Compare People v. Mayoff* (1986) 42 Cal.3d 1302, 1312, *with California v. Ciraolo* (1986) 476 U.S. 207, 214.) Other cases highlight the differences between the federal and state clauses. (*Compare People v. Krivda* (1971) 5 Cal.3d 357, 367 (finding a reasonable expectation of privacy against police scrutiny of garbage placed for pickup) *aff'd*, *People v. Krivda* (1973) 8 Cal.3d 623, *with California v. Greenwood* (1988) 486 U.S. 35, 40 (holding the opposite).)

Similarly, Article I, § 13 has no third-party doctrine, so when people share personal information with third parties, it does not vitiate their reasonable expectation of privacy. Thus, while the Fourth Amendment does not require a court order to obtain certain bank records, (*United States v. Miller* (1976) 425 U.S. 435), and phone records, (*Smith v. Maryland* (1979) 442 U.S. 735), California's Constitution

does. (*See Burrows v. Superior Court* (1974) 13 Cal.3d 238, 245 (bank statements); *People v. Blair* (1979) 25 Cal.3d 640, 652, 654–55 (credit card records and phone records); *People v. Chapman* (1984) 36 Cal.3d 98, 108 (name of unlisted phone subscriber); *People v. McKunes* (1975) 51 Cal.App.3d 487, 490–91 (phone records).)

B. The program is a search because people have a reasonable expectation of privacy in their Smart Meter data.

Under Article I, § 13, a search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. (*See People v. Camacho* (2000) 23 Cal.4th 824, 830–31 (quotation omitted); *see also Katz v. United States* (1967) 389 U.S. 347 (Harlan, J., concurring).)

1. Leading cases protect the privacy of home electricity data.

California courts have not addressed the expectation of privacy in the context of smart meter electricity data. A federal court, however, has.

In *Naperville Smart Meters Awareness v. City of Naperville* (7th Cir. 2018) 900 F.3d 521, plaintiffs challenged a public utility's collection of energy usage information via smart meters. The court held this constituted a "search," explaining: "The ever-accelerating pace of technological development carries serious privacy implications. Smart meters are no exception. Their data, even when collected at fifteen-minute intervals, reveals details about the home that would be otherwise unavailable to government officials with a physical search." (*Id.* at p. 525–27.) The public utility was using "a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion." (*Naperville, supra*, 900 F.3d at p. 526 (citing *Kyllo v. United States* (2001) 533 U.S. 27, 31–32).)

Naperville rested on U.S. Supreme Court decisions recognizing that police can use powerful new technologies in a manner akin to a paradigmatic physical door-to-door search. *Naperville* cited *Kyllo v. United States*, which held that police conducted a "search" under the Fourth Amendment when they used a thermal imaging device to detect cannabis cultivation inside a home. 533 U.S. at p. 40. *Kyllo* emphasized that

constitutional protections must consider modern developments: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." (*Id.* at pp. 33–34.)

Naperville also cited *Carpenter v. United States* (2018) 585 U.S. 296, 310, which held that police conducted a "search" when they seized historical cell site location information ("CSLI") from a wireless phone carrier. The Court explained that phone users have a reasonable expectation of privacy in their CSLI (*id.* at pp. 310–13.) and this expectation is not reduced by its disclosure to their third-party carriers. (*Id.* at pp. 314–15.) The Court reasoned that the "comprehensive reach" of this data was "deeply revealing," and that its collection was "inescapable and automatic." (*Id.* at p. 320.) The Court also emphasized the "seismic shift in digital technology" that enabled the "ever alert" and "exhaustive" surveillance at issue. (*Id.* at p. 313–14.)

SMUD's smart meters are a "seismic shift in digital technology." (*Ibid.*) They are also "automatic," "ever alert," and have "comprehensive reach." (*Id.* at pp. 313–14, 320.) They continuously scoop up data from SMUD's 650,000 customers every 15 minutes, and wirelessly and automatically send it multiple times per day to SMUD, which retains it for years. (*See supra* pp. 8–10.) The 15-minute interval collection is nearly a 3,000-fold increase over the prior analog meters that provided only a monthly snapshot, and a 700-fold increase when the smart meter data is observed in one-hour intervals.[4] And the granularity of SMUD's data is ever increasing.[5]

SMUD's smart meters are "inescapable." SMUD has installed them for 99.9% of its 650,000 customers, who have no reasonable alternative to SMUD. (*See supra* pp. 9–

---

[4] The arithmetic is simple: Four collections/hour x 24 hours/day x 30 days/month = 2,880 collections/month. Likewise, 24 observations/day x 30 days/month = 720 observations/month.

[5] *See* Request for Judicial Notice: Sac. Mun. Util. Dist., "SMUD announces $50 million grant to support advanced smart grid technologies," Oct. 18, 2023, https://www.smud.org/Corporate/About-us/News-and-Media/2023/2023/SMUD-announces-$50-million-grant-to-support-advanced-smart-grid-technologies (Record 1908).

10.) Moreover, SMUD transitioned customers to smart meters by default and imposed extra fees to discourage opt-outs. Some customers cannot opt out. (*See supra* p. 7.)

SMUD's smart meters, coupled with powerful software, allow the utility to "reveal[] details about the home that would be otherwise unavailable to government officials with a physical search." (*Naperville*, *supra*, 900 F.3d at p. 527.) This is precisely why law enforcement considers SMUD a critical part of the law enforcement "team" and why it would supposedly be "problematic" if SMUD did not make this data available by way of their analysts' opinions. (*See supra* pp. 12–13.)

By its own admission, SMUD undertakes a "painstaking process" of searching, sorting, filtering, visualizing, and analyzing its customers' smart meter interval data for law enforcement. (*See supra* pp. 10–11.) Then, SMUD offers opinions to law enforcement about what customers might be doing in their home. SMUD analysts, for instance, opine if a customer has a particular level or "pattern" of usage, is "Asian," might be mining cryptocurrency, or is doing something "7pm to 7am" that SMUD feels, often incorrectly, might be untoward, like growing cannabis. (*See supra* pp. 15–16.)

Petitioners' expert, Dr. Wicker, details the well-recognized home privacy concerns raised by smart meters. (*See supra* p. 8.) His report reviews the many studies that demonstrate that smart meter data can reveal what people are doing in their home — including when they are active or away; when they are sleeping or awake; their family size; and deeply personal demographic information. (*Ibid*.) He even explains that smart meter data can be used to infer "showering"— providing insight into "intimate" domestic behavior that shows a search has occurred. (*Kyllo*, *supra*, 533 U.S. at p. 38 (technology used to conduct a search "might disclose … at what hour each night the [resident] of the house takes [their] daily sauna and bath").)

2. The privacy of home electricity data is protected by "positive law."

The need to keep home electricity data private is also reflected in California's "positive law." (*See Hill v. NCAA* (1994) 7 Cal.4th 1, 36 (looking to "positive law,"

including common law, statutes, and ballot arguments, to inform whether the California Constitution's Privacy Clause protects a privacy interest); *see also Carpenter*, *supra*, 585 U.S. at p. 402 (Gorsuch, J., dissenting) ("positive law may help establish a person's Fourth Amendment interest").)

In 2001, for instance, the California Narcotics Officers' Association ("CNOA") petitioned the California Public Utilities Commission ("CPUC") to relax its privacy protections because it "slow[ed] down their everyday work." (Cal. P.U.C. Ruling No. 01-07-032 (July 2, 2001) at pp. 2-3 [Record 1888–1889].) The CPUC prohibited investor-owned electric utilities (*e.g.*, PG&E) from releasing customer data unless law enforcement obtained a warrant or a judicially approved subpoena. (*Id.* at 1887.) In denying the CNOA's request, the CPUC highlighted "privacy rights based on Article I, §13 of the California Constitution," and approvingly cited the aforementioned California Supreme Court decisions in *Blair* and *Chapman*. (*Id.* at 1900–1901.)

The CPUC also referenced existing "statutes protecting [] confidentiality," including Public Utilities Code, § 394.4. (*Id.* at 1902.) That provision requires the CPUC to adopt rules to guarantee that "[c]ustomer information shall be confidential unless the customer consents in writing," and that generic information can be disclosed only if it would not "reveal customer specific information." (Pub. Util. Code, § 394.4(a).)[6] Hence, the Legislature sought to preserve the privacy of utility data.

In 2010, in anticipation of the wider rollout of smart meters, the Legislature passed Public Utilities Code §§ 8380 and 8381, which protect customer information when utilities, like SMUD, have an "advanced metering infrastructure" such as smart meters. These provisions command that the covered utilities, with narrow exceptions, "shall not share, disclose, or otherwise make accessible to any third party a customer's electrical consumption data." (Pub. Util. Code, §§ 8380(b)(1) & (f)(3); *id.* §§ 8381(b)(1)

---

[6] The statute also contains an exception not applicable here, but even that exception requires a court order or subpoena for disclosure of customer usage information. *See* Pub. Util. Code § 588.

& (f)(3).) The Senate Report explained, "[c]onsumption data can reveal sensitive personal information about a customer's schedule and intimate details about their lives such as their medical needs and personal habits."[7]

In 2020, the Legislature amended these statutes to bar utilities from disclosing data to any immigration authority "without a court-ordered subpoena or judicial warrant." (Pub. Util. Code, §§ 8380(e) & 8381(e).) The Assembly Report noted, "[s]mart meters give customers, and utilities, a snapshot of their energy usage throughout the day" and could reveal "where a person lives, the number of people in a household, and their comings and goings."[8]

Finally, SMUD's own policies recognize the privacy of its customers' data: "Customer information," including "electricity usage," is "Sensitive and Confidential." (Record 703–707.) The policies also require customer consent to disclose "sensitive and confidential customer information to a third party for non-SMUD business purposes," absent narrow exceptions. (Record 709.) SMUD underscores the need to maintain privacy by touting that "SMUD's wireless network uses the same types of security as the Department of Defense and the online banking industry." (Record 492.)

In sum, the Court should find that SMUD's customers have a reasonable expectation of privacy in their electrical consumption data gathered by smart meters, and that SMUD and law enforcement's surveillance program constitutes a search.

C. Respondents' systematic, suspicionless search of customer energy usage data is unreasonable.

Suspicionless searches—like Respndents' dragnet trawling through SMUD

---

[7] Sen. Energy, Utilities & Communications Com., Analysis of Sen. Bill No. 1476 (2009-2010 Reg. Sess.) April 2, 2010, p. 2, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=200920100SB1476.

[8] Assem. Com, on Utilities & Energy, Analysis of Assem. Bill No. 2788 (2019-2020 Reg. Sess.) May 27, 2020, p. 3. https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB2788.

customers' sensitive and confidential data—are "per se unreasonable … subject only to a few specifically established and well-delineated exceptions." (*People v. Laiwa* (1983) 34 Cal. 3d 711, 725; *People v. Superior Court* (2006) 143 Cal.App.4th 1183, 1196 (quoting *Katz*, *supra*, 389 U.S. at p. 357); *accord Al Haramain Islamic Foundation, Inc. v. U.S. Treasury Dept.* (9th Cir. 2011) 686 F.3d 965, 990.) The government bears the burden of proving "by a preponderance of the evidence that [a] search falls within an exception …." (*People v. Marquez* (2019) 31 Cal.App.5th 402, 409.)

SMUD's sharing of lists, opinions, and tips with law enforcement constitutes a "search." In *Naperville*, the court found that the mere collection of smart meter data by a public utility was a "search." (*Supra*, 900 F.3d at pp. 525–27.) SMUD's conduct is far more intrusive. SMUD does not just collect data from smart meters. With its powerful software, SMUD searches, sorts, filters, visualizes, and analyzes entire zip codes' worth of its customers' data, in the absence of suspicion. (*See supra* pp. 8–10.)

SMUD's analysts then give law enforcement the names and addresses of customers, how much electricity they used in the past 30 days, and often opinions about what they might be doing in their home. (*See supra* pp. 8–10.) SMUD has done so for a decade for multiple law enforcement agencies and continues to do so quarterly for the Sacramento Police. (*See supra* pp. 10–13.) The first search is of virtually all customers in the 23 zip codes that cover the City of Sacramento. (*See supra* pp. 10–11.) SMUD's analysts are not unwitting data responders, but rather are part of the law enforcement "team." For instance, they invite the police to "send me a request" for a specific property where the subscribers are "Asian"; they coach law enforcement on how to fill out the form to obtain a zip code list; and they encourage police to conceal from SMUD's own customers the depth of SMUD's involvement. (*See supra* pp. 16–17.)

SMUD's disclosures invade the privacy of customers' homes. (*See supra* pp. 7–8.) The whole exercise is the digital equivalent of a door-to-door search of an entire city. The home lies at the "core" of constitutional privacy protection. (*Naperville*, *supra*, 900 F.3d at p. 525; *Kyllo*, *supra*, 533 U.S. at p. 31; *see also Caniglia v. Strom*

(2021) 593 U.S. 194, 198 (the "very core" of the Fourth Amendment is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion").) Article I, § 13 is even more protective of Californians' privacy. (*Mayoff*, *supra*, 42 Cal.3d at p. 1312; *Krivda*, *supra*, 5 Cal.3d at 367.)

Law enforcement never obtain a warrant to get SMUD's customers' data. Neither do they have individualized suspicion of any crime being committed. SMUD turns over information upon a so-called "official" request by law enforcement. (*See supra* p. 17.) A mere text message from law enforcement asking for a "tip" is sufficient to unlock SMUD's trove of customer data. (*See supra* p. 12.)

In *Naperville*, while the court found a reasonable expectation of privacy and a search, it ultimately ruled the search was reasonable because the utility had "no prosecutorial intent," and "no law enforcement … collect[ed] and review[ed] the data." (*Supra*, 900 F.3d at 528–29.) The court, however, cautioned that its decision "might change if the data was more easily accessible to law enforcement …." (*Ibid.*)

Here, the whole purpose of the surveillance program is to give law enforcement access to residents' sensitive utility data. Police rely on lists from SMUD before initiating investigations into customers who were under no prior suspicion. (*See* Record 1356, 1367 (returned warrant noting SMUD provided information, and only then did the officer "initiate[] an investigation"). The sharing is all about prosecutorial intent. After SMUD points a finger at a customer, Sacramento Police sends them a letter (called a "nastygram[]" by one SMUD analyst) stating: "the Property Owner and/or Current Occupant may be subject to criminal prosecution, administrative penalties, and/or a civil penalty." (*See supra* pp. 13–14.)

The Court should stop this rogue and unreasonable dragnet. Despite sworn statements in warrant applications declaring that SMUD analysts have "never incorrectly assessed" data, they have recurringly done just that. (*See supra* pp. 14–16.) Indeed, one Sacramento Police affiant testified that SMUD's data was about as productive as "driv[ing] around East Sacramento and roll[ing] down my windows and

try[ing] to smell something." (Record 1343.) At deposition, he described showing up at customers' homes only to find electricity consumption resulting from a large fish tank, exotic plants, or a man cave. (*See supra* p. 14; Record 1339–1344.) Customers have told police that they felt "criminalized" and "pissed off" about the police showing up. When customers complained, SMUD resorted to trying to minimize its decade-long role in the dragnet. (*See supra* p. 16; Record 863, 1220–1221 ("leave SMUD out of it").)

No homeowner should be called a "liar" by a sheriff's deputy when they honestly deny growing cannabis, as happened to Petitioner Nguyen on account of SMUD's false tip. (*See supra* p. 15.) Nor should anyone ever have to walk out of their home in their underwear to blaring sirens and drawn guns, as declarant Decker was forced to do because SMUD sent a list and then incorrectly told law enforcement that "4 to 5 [grow] lights are being used from 7pm to 7am." (*See supra* pp. 15–16.)

Petitioners respectfully ask the Court to find: (1) SMUD's customers have a reasonable expectation of privacy in their electrical consumption data collected by SMUD's smart meters, and so the challenged home energy surveillance program is a search; and (2) this search is suspicionless and thus per se unreasonable, and accordingly a violation of Article I, § 13.

II. Respondents' dragnet program violates a state privacy statute.

As noted above, in 2010, the Legislature passed Public Utilities Code § 8381. (*See supra* pp. 22–23.) The pertinent provision provides: "A local publicly owned electric utility shall not share, disclose, or otherwise make accessible to any third party a customer's electrical consumption data,[9] *except* as provided in subdivision (f) or upon consent of the customer." (Pub. Util. Code, § 8381(b)(1) (emphasis added).) The former exception provides for disclosure "as required under state or federal law." (*Id.*

[9] An earlier part of the provision defines "electrical consumption data" as "data about a customer's electrical usage that is made available as part of an advanced metering infrastructure, and includes the name, account number, or residence of the customer." *Id.* at (a).

at (f)(3).) Respondents violate this statute and cannot prove their disclosure of customer data meets any exception.

A. Respondents violate Public Utilities Code § 8381.

SMUD is subject to Public Utilities Code § 8381's privacy protections. It is a "local publicly owned utility" because it was formed under the Municipal Utilities District Act. (Pub. Util. Code, § 224.3; *see supra*, p. 7.) The data that SMUD collects and turns over is "made available as part of an advanced metering infrastructure" because 99.9% of its customers have smart meters. (Record 432 (describing smart meters as "advanced metering infrastructure"), 244–45.)

Finally, there is no doubt that under the challenged dragnet program, SMUD has "share[d], disclose[d], or otherwise ma[de] accessible to [a] third party a customer's electrical consumption data." (*See supra* pp. 8–13.) At a minimum, SMUD admits it "has given customer data to Sacramento Police Department." (Record 809 ¶7).

B. Respondents bear the burden of proving an exception to § 8381.

Public Utilities Code § 8381(b)(1) provides exceptions to its non-disclosure command. Specifically, it bars disclosure "*except* as provided in subdivision (f) or upon the consent of the customer." (Emphasis added.) Subdivision (f)(3) provides for disclosures "required under state or federal law."

Respondents bear the burden of proving any of these exceptions. When, as here, a statute contains an exception to a rule, and it is an "excuse merely" as opposed to "part of the [rule's] definition," then it is an "affirmative defense." (*Brentwood v. Central Valley Water Bd.* (2004) 123 Cal.App.4th 714, 725–26; *see, e.g., id.* (in a statute limiting waste discharge, the exception for natural disasters is an affirmative defense); *Jones v. Credit Auto Ctr* (2015) 237 Cal.App.4th Supp. 1, 10–11 (in a statute on warranty of merchantability, the exception for a buyer's conduct is an affirmative defense); *see generally People v. Dawson* (2021) 69 Cal.App.5th 583, 591 ("where a statute first defines an offense in unconditional terms and then specifies an exception

to its operation, the exception is an affirmative defense").) Here, Respondents cannot meet their burden to prove that they comply with an applicable exception.

C. Respondents cannot show police requests and SMUD disclosures are "relative to an ongoing investigation."

A California Public Records Act ("CPRA") provision states: "disclosure of the name, utility usage data, and the home address of a utility customer of a local agency shall be made available … [u]pon … the request of a law enforcement agency relative to an ongoing investigation." (Government Code § 7927.410(c) (formerly § 6254.16(c)).)

This CPRA provision reformed prior law. Consumer data held by a public utility was historically subject to the CPRA. (*See, e.g.*, *New York Times v. Superior Court of Santa Barbara* (1990) 218 Cal.App.3d 1579.) However, in 1997, the Legislature—in response to incidents in which utilities disclosed customer information to malevolent actors—amended the CPRA to prohibit public utilities from disclosing consumer information, except in narrow instances, including for law enforcement requests "relative to an ongoing investigation." (Gov. Code § 7927.410(c).)

Should Respondents assert this exception, which SMUD pre-prints on its Law Enforcement Customer Request Form, they cannot meet their burden of proving it applies. In interpreting a statute, California courts look to "the language used" and construe it "in context" of "statutory sections relating to the same subject." (*People v. Valencia* (2017) 3 Cal.5th 347, 357–58.) Where ambiguity remains, courts use "other aids, such as the statute's purpose, legislative history, and public policy." (*Jones v. Torrey Pines* (2008) 42 Cal.4th 1158, 1163.)

The term "ongoing investigation" is not defined by Government Code § 7927.410. Nor has a California court interpreted it. But it has a plain meaning. *Merriam-Webster* defines "ongoing" as "being actually in process" or "continuing." Merriam-Webster.[10] Law enforcement investigations are not "in process" or

---

[10] *Ongoing* Merriam-Webster.com Dict., https://www.merriam-webster.com/dictionary/ongoing.

"continuing" when, as here, law enforcement has no suspicion prior to making a request to SMUD that a specific residence or person is suspected of a violation of law.

Case law in related areas supports this dictionary definition. In *ACLU v. Superior Court* (2017) 3 Cal.5th 1032, the California Supreme Court interpreted the CPRA exception for "[r]ecords of … investigations." (Gov. Code § 7923.600.) At issue was whether the exception allowed police to withhold automated license plate reader ("ALPR") data. The Court held that "bulk collection of raw ALPR data" did not constitute "records of investigations." (*ACLU*, *supra*, 3 Cal.5th at p. 1042.) It reasoned that ALPR scans are "not conducted as part of a targeted inquiry into any particular crime or crimes," but rather "with an expectation that the vast majority of the data collected will prove irrelevant for law enforcement purposes." (*Ibid.*) Further, the Court distinguished (i) records showing "an informant's choice to come forward, an investigator's choice to focus on particular individuals, [or] the choice of certain investigatory methods," which would be sufficiently individualized to be exempt, from (ii) "data … collected *en masse*," which would not. (*Id.* at p. 1041.)

Similarly, the federal Stored Communications Act allows disclosure of customer data only where "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to *an ongoing criminal investigation*." (18 U.S.C. § 2703(d) (emphasis added).) Courts reject government applications that fail to show a targeted inquiry. (*See, e.g.*, *In re Applications* (D.D.C. 2016) 206 F.Supp.3d 454, 456–57 (denying access to 21 electronic accounts because the application rested on "conclusory statements," such access was "unlikely to be the first step in a criminal investigation," and the statute did not allow "government fishing expeditions"); *United States v. Moreno-Vasquez* (D. Ariz. Mar. 11, 2020) 2020 WL 1164970, at p. 3 (suppressing evidence collected under a 2703(d) order that rested on "conclusory statements" instead of "specific facts").)

Likewise, in *Polkey v. Transtecs Corporation* (11th Cir. 2005) 404 F.3d 1264, a

federal appellate court considered a statute that protected employees from polygraph tests absent an "ongoing investigation." The court held the exemption did not apply where "the company aimed to test all of its employees" when investigating a particular incident, reasoning that "[t]o allow such blanket testing under the ongoing investigation exemption would vitiate [the statute's] requirement of reasonable suspicion as to each individual employee." (*Id.* at p. 1270.)

Moreover, the legislative history shows the "ongoing investigation" exception was intended to be narrow and to foreclose disclosure to law enforcement upon mere request. When the reform bill was first introduced in February 1997, the proposed exception said: "[U]pon court order *or the request* of a law enforcement agency." (Record 1437 (emphasis added).) As it progressed through the Senate, a March 31, 1997, handwritten committee markup questioned, "Why should law enforcement or other govt agency get this info upon mere request?" (Record 1441.) The final bill that passed added the words "relative to an ongoing investigation" to ensure that law enforcement could not just issue a demand and thereby obtain private utility information. (*See* Gov. Code § 7927.410(c); Record 1459.)

Here, SMUD shares data whenever law enforcement asks. Their conduct is an *en masse* dragnet surveillance. Their lists are bulk, in one case including more than 10,000 customers. (*See supra* pp. 11–12, Record 1555–1769.) Their conduct is nothing more than a "fishing expedition." It is not a targeted inquiry in an ongoing investigation. As previously noted, SMUD's sharing often occurs based on a "Law Enforcement Customer Information Request" form. (*See supra* p. 17.) SMUD pre-prints on the top that the request is "part of an ongoing investigation" and cites Government Code § 6254.16(c) (now § 7927.410(c)). (*See supra* p. 17.) But Respondents do not have or apply any criteria to determine if a request is actually part of an "ongoing investigation." (*See supra* p. 17; Record 842–843; 854; 1218–1219; 1254–1257.) The form contains just a threadbare recitation of the statute's magic words.

Moreover, Sacramento Police's Mendoza quarterly asks SMUD to search all of

its customers in all 23 zip codes covering the City of Sacramento. (*See supra* p. 10–12.) But police officers testified that their investigations do not begin *until* they receive SMUD's lists. (*See supra* pp. 13–14.) In a supporting affidavit to a search warrant, a police officer stated that he got the SMUD zip code list first and only then "initiated an investigation" into that home. (*See supra* p. 13, Record 1355–1356.) Plainly, getting customer data based on a suspicionless request is not a request relative to an "ongoing investigation." SMUD simply searches and turns over lists, opinions, tips, and customer data whenever law enforcement requests. Further, sometimes even before law enforcement makes a request, a SMUD analyst sends law enforcement a text asking them to "send me a request." (*See supra* p. 12, Record 1298.) This is precisely what the legislative history shows was *not* intended.

D. Respondents cannot show police requests and SMUD disclosures are "upon the consent of the customer."

Public Utilities Code § 8381(b)(1) exempts disclosures "upon the consent of the customer." Respondents cannot prove they have customers' consent to disclose their data to police. (*See* Civ. Code §§ 1580, 1565 ("The consent of the parties to a contract must be: 1. Free; 2. Mutual; and, 3. Communicated by each to the other").)

Here, consent is not free because SMUD is the only electricity service provider in the region, so residents cannot meaningfully refuse. (Record 1316; 555.) Nor is it mutual because no reasonable customer could interpret SMUD's policy to authorize the dragnet home energy surveillance program. Nor does SMUD require customers to enter into a contract before receiving service. (*See Preliminary Statement*, Rates, Rules, and Regulations Effective in 2023, SMUD Resol. No. 23-09-09.)[11] Moreover, the utility's own employees concede SMUD does not get, and customers do not give, consent to this dragnet home energy surveillance program. (Record 1251, 1326.)

The mere existence of SMUD's "Privacy Policy" likewise does not demonstrate

---

[11] Available at https://www.smud.org/-/media/Documents/Corporate/About-Us/Company-Information/Reports-and-Documents/GM-Reports/2023/SMUD-Resolution-No-23-09-09.ashx.

consent. For online terms to indicate user consent, SMUD, at the very least, must prove that (1) it provides "reasonably conspicuous notice of its terms"; and (2) the customer "takes some action" like clicking a button or checking a box that unambiguously manifests assent to those terms. (*Berman v. Freedom Fin. Network, LLC* (9th Cir. 2022) 30 F.4th 849, 856–57 (applying California state law).) Merely providing a hyperlink is "insufficient to give rise to constructive notice." (*Nguyen v. Barnes & Noble Inc.* (9th Cir. 2014) 763 F.3d 1171, 1178–79 (applying California state law).) Importantly, there is no mechanism by which a customer can give consent to SMUD when signing up for service. (*See generally* Record 1405–1409, 1423–1431.) Furthermore, 40% of SMUD's customers started service before SMUD even adopted its bottom-of-page link to its "Privacy Policy" — leaving them with no meaningful opportunity to consent or be presented with the option to refuse. (*See* Record 803.)

III. Petitioners have standing.

Each Petitioner has standing on at least three grounds.

Petitioners have public interest standing because they seek a writ of mandate to hold Respondents accountable for their violations of all customers' statutory and constitutional privacy rights. "The *raison d'être* of taxpayer standing, as well as the related doctrine of public interest standing in mandamus proceedings, is to confer standing on the public at large to hold the government accountable to fulfill its obligations to the public." (*People for the Ethical Operation of Prosecutors v. Spitzer* (2020) 53 Cal.App.5th 391, 395–96; *Save the Plastic Bag Coalition v. City of Manhattan Beach* (2011) 52 Cal.4th 155, 166.)

Petitioners also have a beneficial interest. (*See* Code Civ. Proc. § 1086; *Save the Plastic Bag Coalition*, *supra*, 52 Cal.4th at pp. 165–66.) SMUD disclosed Petitioner Nguyen's customer energy usage data, which led law enforcement to target and harass him. (Record 143 ¶¶ 3–5.) He seeks to ensure that neither he nor anyone else is subjected to similar future intrusions. (Record 144 ¶ 8.) Petitioner Khoja is a SMUD customer, a resident of the City of Sacramento, and a longtime advocate for the Asian

community. (Record 151 ¶¶ 1–2.) He advises people and businesses in the legal cannabis industry in California. (*Id.* ¶ 1.) Khoja seeks to reform punitive laws surrounding drug possession and cultivation because he believes enforcing these laws has created disproportionate impacts on Asian and other minority communities. (*Id.* ¶ 3.) Petitioner AALN's mission is to build power within the Asian community in Sacramento and advance social justice. (Record 149 ¶ 2.) It seeks to prevent over-policing of the Asian community, by protecting the privacy of SMUD customers' data and ending the discriminatory effects of the dragnet program. (*Id.* ¶¶ 3–4.)

Petitioners also have standing because they paid a tax within a year of the filing of this suit that directly or indirectly funds one or more of the Respondents. (Code Civ. Proc. § 526a; *A.J. Fistes Corp. v. GDL Best Contractors, Inc.* (2019) 38 Cal.App.5th 677, 692-694; *see also Taxpayers for Accountable School Bond Spending v. San Diego Unified Sch. Dist.* (2013) 215 Cal.App.4th 1013 (organizations have taxpayer standing when a member has paid the tax).)

The City levies a utility tax on every SMUD customer within the City, and Petitioners Khoja and AALN (through its members) paid it. (Record 304–305, 151 ¶ 5, 149 ¶ 5.) SMUD collects and remits the tax to the City. (Record 304–305.)

SMUD also collects a "State Surcharge" levied under Revenue & Taxation Code §§ 40016-40036, and Petitioners Khoja, Nguyen, and AALN (through its member) paid this tax. (Record 151 ¶ 5, 144 ¶ 9, 149 ¶ 5.) SMUD remits it to the State. (Record 304.) The State places it in the Energy Resources Programs Account, which funds the California Energy Commission. Rev. & Tax. Code § 40182. SMUD received $191,759 from the California Energy Commission. (Record 304–305, 555, 562–563.)

IV. Petitioners are entitled to relief stopping Respondents from violating the California Constitution and state law.

Writ relief is appropriate "to compel the performance of an act which the law specially enjoins …." (Code Civ. Proc. § 1085(a).) "Mandamus will lie to compel a public official to perform an official act required by law." (*Common Cause v. Bd. of*

Supervisors (1989) 49 Cal.3d 432, 442; *see also* Code Civ. Proc. § 525.) Respondents, by means of their dragnet program, are violating their mandatory duties under the California Constitution and state privacy laws. (*Supra* Sections I & II.) Petititioners respectfully ask this Court to command:

(1) Respondents SMUD and Lau to maintain the confidentiality of SMUD's customers' names, addresses, and electricity consumption (and any opinions derived therefrom), and to discontinue making the same available to any law enforcement agency, such as by disclosing lists (such as zip code lists) of multiple customers or properties, absent a prior showing by law enforcement of a prior individualized suspicion of wrongdoing.

(2) Respondents City of Sacramento and Lester to respect the confidentiality of SMUD's customer information and discontinue requesting names, addresses, or electricity consumption (and any opinions derived therefrom) from SMUD, including lists of the same (such as zip code lists), absent a prior showing by law enforcement of individualized suspicion of wrongdoing.

(3) Such other relief as the Court deems proper.

CONCLUSION

Petitioners respectfully request that this Court grant the writ.

Dated: July 18, 2025

Respectfully submitted,

/s/ Aaron Mackey

SAIRA HUSSAIN (SBN 300326)
AARON MACKEY (SBN 286647)
F. MARIO TRUJILLO (SBN 352020)
ADAM SCHWARTZ (SBN 309491)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Email: saira@eff.org
amackey@eff.org
mario@eff.org
adam@eff.org

MONTY AGARWAL (SBN 191568)
RACHEL CHANIN (SBN 229253)
VALLEJO | ANTOLIN | AGARWAL | KANTER LLP
3021 Citrus Circle, Suite 220
Walnut Creek, CA 94598
Telephone: (925) 951-6970
Email: magarwal@vaakllp.com
rchanin@vaakllp.com

Attorneys for Petitioners