NO. 16-3766

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

NAPERVILLE SMART METER AWARNESS,
AN ILLINOIS NOT-FOR-PROFIT CORPORATION

PLAINTIFF-APPELLANT,

V.

CITY OF NAPERVILLE,

DEFENDANT-APPELLEE.

On Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division
Case No. 11-cv-09299
The Honorable John Z. Lee, District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND PRIVACY INTERNATIONAL IN SUPPORT OF PLAINTIFF-APPELLANT NAPERVILLE SMART METER AWARENESS AND REVERSAL

David Greene (*Counsel of Record*)
Jamie Williams
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
davidg@eff.org

Caroline Wilson Palow
Scarlet Kim
PRIVACY INTERNATIONAL
62 Britton Street
London EC1M 5UY
United Kingdom
Telephone: +44 (0) 20 3422 4321
caroline@privacyinternational.org

Attorneys for *Amici Curiae*
Electronic Frontier Foundation
and Privacy International

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 16-3766

Short Caption: Naperville Smart Meter Awareness v. City of Naperville

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Electronic Frontier Foundation

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Electronic Frontier Foundation, Privacy International

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

None.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

None.

Attorney's Signature: s/ David Greene Date: 2/28/2017

Attorney's Printed Name: David Greene

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** X **No** ____

Address: 815 Eddy Street
San Francisco, CA 94109

Phone Number: (415) 436-9333 Fax Number: (415) 436-9993

E-Mail Address: davidg@eff.org

rev. 01/15 GA

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 16-3766

Short Caption: Naperville Smart Meter Awareness v. City of Naperville

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Electronic Frontier Foundation

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Electronic Frontier Foundation, Privacy International

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

None.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

None.

Attorney's Signature: s/ Jamie Lee Williams Date: 2/28/2017

Attorney's Printed Name: Jamie Lee Williams

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: 815 Eddy Street
San Francisco, CA 94109

Phone Number: (415) 436-9333 Fax Number: (415) 436-9993

E-Mail Address: jamie@eff.org

rev. 01/15 GA

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 16-3766

Short Caption: Naperville Smart Meter Awareness v. City of Naperville

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Electronic Frontier Foundation

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Electronic Frontier Foundation, Privacy International

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

None.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

None

Attorney's Signature: s/ Lee Tien Date: 2/28/2017

Attorney's Printed Name: Lee Tien

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: 815 Eddy Street
San Francisco, CA 94109

Phone Number: (415) 436-9333 Fax Number: (415) 436-9993

E-Mail Address: tien@eff.org

rev. 01/15 GA

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 16-3766

Short Caption: Naperville Smart Meter Awareness v. City of Naperville

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Privacy International

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Electronic Frontier Foundation, Privacy International

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

None.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

None.

Attorney's Signature: s/ Scarlet Sue Kim Date: 2/28/2017

Attorney's Printed Name: Scarlet Sue Kim

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** _____ **No** X

Address: 62 Britton Street
London United Kingdom EC1M5UY

Phone Number: +44 (0) 20 3422 4321 Fax Number: n/a

E-Mail Address: scarlet@privacyinternational.org

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 16-3766

Short Caption: Naperville Smart Meter Awareness v. City of Naperville

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

[ ] **PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.**

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P 26.1 by completing item #3):

Privacy International

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Electronic Frontier Foundation, Privacy International

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

None.

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

None.

Attorney's Signature: s/ Caroline Elizabeth Wilson Palow Date: 2/28/2017

Attorney's Printed Name: Caroline Elizabeth Wilson Palow

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). **Yes** ____ **No** X

Address: 62 Britton Street
London United Kingdom EC1M5UY

Phone Number: +44 (0) 20 3422 4321 Fax Number: n/a

E-Mail Address: caroline@privacyinternational.org

rev. 01/15 GA

RULE 26.1 DISCLOSURE STATEMENT

The Electronic Frontier Foundation, a non-profit public advocacy organization, has not appeared earlier in this case and no attorney from any other organization or law firm has appeared, or is expected to appear, on behalf of the Electronic Frontier Foundation in this case. The Electronic Frontier Foundation states that it does not have a parent company, subsidiary or affiliate, and does not issue shares to the public.

Privacy International, a non-profit public advocacy organization, has not appeared earlier in this case and no attorney from any other organization or law firm has appeared, or is expected to appear, on behalf of Privacy International in this case. Privacy International states that it does not have a parent company, subsidiary or affiliate, and does not issue shares to the public.

Dated: February 28, 2017 By: */s/ David Greene*

David Greene
ELECTRONIC FRONTIER FOUNDATION

Counsel of Record for *Amici Curiae* pursuant to Circuit Rule 3(d)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online world for roughly 25 years. With roughly 36,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF has filed *amicus* briefs with this Court in numerous cases involving the application of constitutional principles to emerging technologies. *See, e.g.*, *U.S. v. Patrick*, 842 F.3d 540 (7th Cir. 2016); *Belleau v. Wall*, 811 F. 3d 929 (7th Cir. 2016); *Backpage.com, LLC v. Dart*, 807 F.3d 229, (7th Cir. 2015); *McCarthy v. Langsenkamp Family Apostolate*, 810 F.3d 456 (7th Cir. 2015); *United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014). EFF also has filed *amicus* briefs with the U.S. Supreme Court in cases applying the Fourth Amendment to new technology. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 565 U.S. 400 (2012).

Privacy International is a nonprofit, non-governmental organization based in London, which defends the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices.

---

[1] No party or party's counsel has authored this brief in whole or in part. No party, party's counsel, or other person has contributed money that was intended to fund preparing or submitting the brief. Plaintiff-Appellant Naperville Smart Meter Awareness ("NSMA") consents to the filing of this brief; Defendant-Appellee City of Naperville does not.

It has litigated, intervened, or filed amicus briefs in cases implicating the right to privacy in the courts of the United States, the United Kingdom, and Europe, including the European Court of Human Rights and the European Court of Justice. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect this right. It also strengthens the capacity of partner organizations in developing countries to identify and defend against threats to privacy.

INTRODUCTION

"Time . . . is what keeps everything from happening at once." Ray Cummings, *The Girl in the Golden Atom*, ch. 5 (1922) (internal quotations omitted).[2]

Time is also why smart meters are different—both quantitatively and qualitatively—from their predecessors, analog meters, in terms of the information captured regarding in-home activities. The district court failed to recognize this, and in so doing, issued a holding that threatens to erode the sacred privacy of the home.

The district court held that Americans have no reasonable expectation of privacy in their aggregate smart meter data as a matter of law. This holding rests on a presumption that aggregate smart meter data is no more informative than the "only one data point per consumer per month"[3] collected from analog meters. But "aggregate" smart meter data is actually *disaggregated by time*. Whereas analog meters provide a single monthly measurement of cumulative household energy use, smart meters—by measuring energy use at much shorter intervals; here, every 15 minutes[4]—provide information regarding not only how much energy was used, but also the time at which it was used. Smart meters thus not only generate far more

---

[2] This saying has been repeated by many, but Ray Cummings is credited with its first use. *See* Wikipedia, *Ray Cummings*, https://en.wikipedia.org/wiki/Ray_Cummings.

[3] Rachel Nuwer, *Why Power Companies Love Smart Meters*, Kellogg Insight (Sept. 8, 2015), https://insight.kellogg.northwestern.edu/article/why-power-companies-love-smart-meters (quoting researcher Ozge Islegen).

[4] The City's smart meters have the capacity to collect data at 5-minute intervals, but it has selected 15-minute intervals at present. Third Amended Complaint ("TAC"), ¶ 38.

data every month than analog meters—here 2,880 meter readings in a 30-day month compared to just one—but the data includes an entirely new variable, *i.e.*, time.

As a result of this time granularity, smart meter data—even in "aggregate" form—constitutes intimate information regarding a person or family's private, in-home activities. A single monthly read of cumulative household energy use does not reveal *how* energy is being used throughout the course of a day. But smart meter data does, and its time granularity tells a story for those who wish to read it. With 15-minute readings, one can see when people go to bed, get up in the morning, or go to school or work; one can see "weekday" and "weekend" patterns; and so on.

Americans reasonably expect details of their private, in-home activities to remain private. The home is "entitled to special [Fourth Amendment] protection as the center of the private lives of our people." *Minnesota v. Carter*, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring). And in the home, "*all* details are intimate details." *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (emphasis in original). Smart meter data, as information about the interior of the home, is entitled the utmost Fourth Amendment protection. Indeed, in *Kyllo*, the Court held that the raw thermal imaging data revealing "the relative heat of various rooms in the home" constituted "intimate details" regarding the interior of the home protected under the Fourth Amendment. *Id.* at 35, n.2. And 15-minute interval smart meter data—data about actual energy use within a home at specific times and reflecting in-home activities—is at least as sensitive as raw thermal imaging data (if not more). The data is thus

entitled to Fourth Amendment protection, regardless of whether or not the City runs any post-collection analysis on the data.

In 2015, roughly 65 million smart meters were installed across the United States, with 88% of them, over 57 million, in homes of American consumers.[5] More than 40 percent of American households currently have a smart meter,[6] and experts predict that number will reach around 80 percent by 2020.[7] The district court's holding that Americans have no reasonable expectation of privacy in aggregate smart meter data as a matter of law threatens the privacy of these 57 million and counting American households. This Court is thus tasked with an important role: addressing "what limits there are upon this power of technology to shrink the realm of guaranteed privacy" in American homes. *See Kyllo*, 533 U.S. at 34.

For the reasons outlined herein, this Court should reverse the district court's flawed conclusion that Americans have no reasonable expectation of privacy in their aggregate smart meter data.

---

[5] U.S. Energy Information Administration, Frequently Asked Questions, *How many smart meters are installed in the United States, and who has them?* (Dec. 7, 2016), https://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3.

[6] Katherine Tweed, *Smart Meters Deliver 1 Billion Data Points Daily*, Greentech Media (Sept. 23, 2013), https://www.greentechmedia.com/articles/read/smart-meters-deliver-1-billion-data-points-daily.

[7] Accenture, *Realizing the Full Potential of Smart Metering*, 21 (2013), https://www.accenture.com/t20160413T230144__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_9/Accenture-Smart-Metering-Report-Digitally-Enabled-Grid.pdf.

ARGUMENT

I. SMART METERS COLLECT DATA FROM INSIDE THE HOME THAT REFLECTS PRIVATE, IN-HOME ACTIVITIES.

A. Smart Meters Collect Data From Inside the Home Regarding How Much Energy Was Used, and at What Time.

Smart meters are electronic utility meters that enable "two-way communication between utilities and consumers."[8] Home utility meters measure aggregate energy consumption for an entire home—*i.e.*, the total amount of electricity consumed by the residence during a given interval. In the age of analog meters, energy use was measured in monthly intervals. Electrical utilities sent "meter readers" out once a month to manually record each household's total monthly consumption; "there was only one data point per consumer per month."[9] In contrast, smart meters automatically collect energy usage data at much higher frequencies and send the data to the utility over the Internet. Smart meters can typically collect data in 5, 15, 30, or 60-minute intervals; the smaller the interval, the higher the granularity of the data collected. Here, Naperville set its smart meters to report a home's energy use every 15 minutes, which equates to 96 readings per day or 2,880 readings in a 30-day month.

Because of its time granularity, smart meter data shows not only *how much* electricity is being used within a home but also *at what time*. Thus, smart meter data is both qualitatively and quantitatively different from analog meter data—

---

[8] *See* U.S. Dep't of Energy, Smartgrid.gov, *Advanced Metering Infrastructure and Customer Systems* (Mar. 13, 2015), https://www.smartgrid.gov/recovery_act/deployment_status/sdgp_ami_systems.html.

[9] Nuwer, *supra* n.3.

shifting from "one data point reflecting *average* monthly use" to between 750 and 8,640 "distinct and time-stamped data points per month that reflect *actual* energy use" at any given time.[10]

B. Because of its Time Granularity, Smart Meter Data—Even in Aggregate Form—Is Far More Intimate Than Cumulative Monthly Analog Meter Data.

The dramatic increase "in the granularity of data available and frequency of collection . . . means that the smallest detail of household life can be revealed" from smart meter data, even in aggregate form.[11]

For example, imagine that you were provided a number reflecting the total amount of steps Alice took over the course of an entire month. From that number, you could infer Alice's average level of daily activity, but you could not infer details of her daily patterns, routines, and habits. If you were instead provided with the total number of steps Alice took every 15 minutes over the course of that month, you would be able to see that Alice typically did not take any steps between 10:15 p.m. and 6:15 a.m., from which you could infer her sleep patterns; that Alice took 50 steps between 3:15 a.m. and 3:30 a.m. on a particular morning, from which you could infer that she got out of bed in the middle of the night; and that Alice typically took between 5,000 and 6,000 steps between 9:00 a.m. and 10:00 a.m. on Saturdays,

---

[10] Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3, ¶ 41 (2008) (emphasis added). Smart meters collecting data at 5-minute intervals collect 288 data points per day or 8,640 data points per 30-day month.

[11] Trans Atlantic Consumer Dialog, *Resolution on Privacy and Security Related to Smart Meters*, 1 (June 2011), https://epic.org/privacy/smartgrid/Smart_Meter_TACD_Resolution_FINAL.pdf.

from which you could infer that she typically went for a long run on the weekend. Without the time granularity, you wouldn't be able to see these details; it would be as if Alice took all the steps at once.

Similarly, whereas an analog meter provides a blunt record of kilowatts consumed over the course of an entire month, a smart meter's granular, "fine-grained usage data indirectly reveals sensitive private information about a customer's activity patterns[.]"[12] The patterns generated by looking at smart meter data over time "can be used to infer the number of people occupying a home, their mundane or illicit habits, and the rhythm of their movements, both in general and on a particular day"[13]—such as when they typically get home from work or that they had guests over on a particular evening. Patterns from aggregate smart meter data can even be used to infer which appliances are functioning in a home at any given time. A refrigerator, a toaster, a coffee maker, and a television set all draw power in different ways.[14] Each source of energy use has a unique "load signature[]"—a "distinct energy consumption pattern[.]"[15] These patterns reveal which devices are using energy at any given time. Just as one might listen to an orchestra recording and pick out different musical instruments based on how they

---

[12] Andres Molina-Markham et al., *Designing Privacy-preserving Smart Meters with Low-cost Microcontrollers,* 2 (2011), https://eprint.iacr.org/2011/544.pdf

[13] Sonia K. McNeil, *Privacy and the Modern Grid*, 25 Harv. J.L. & Tech. 199, 205 (2011).

[14] *See* Splunk Blogs: Security, *Smart Grid Data—the 'wild west' of privacy rights* (May 27, 2011), http://blogs.splunk.com/2011/05/27/smart-grid-data-the-wild-west-of-privacy-rights/ (illustrating spikes in energy use from various appliances).

[15] McNeil, *supra* n.13, at 204.

sound, one can look at aggregate energy use data and pick out different appliances based on the energy consumption patterns.

By assessing these patterns, aggregate smart meter data collected from Alice's home in 15-minute intervals could be used to infer whether she tends to cook microwavable meals or meals on the stove; whether she cooks breakfast; whether and how often she uses exercise equipment, such as a treadmill; whether she has an in-home alarm system; when she typically takes a shower; if she has a washer and dryer, and how often she uses them; and whether she turns on the lights "at odd hours, such as in the middle of the night[.]"[16] Her smart meter data could even disclose the presence of specialized medical equipment.[17] Thus, "mining long periods" of Alice's smart meter data could be used to "uncover indications of illness or changing lifestyle."[18]

As the Illinois Attorney General recognized in a consumer alert issued last year,[19] this information could be used to paint an intimate portrait of Alice's life: she "tends to arrive home shortly after the bars close"; she "is a restless sleeper and is sleep deprived"; she "leaves late for work"; she "often leaves appliances on while

---

[16] Ann Cavoukian, et al., *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, 3 Identity in the Info. Society 2, 275, 284 (Apr. 20, 2010), https://link.springer.com/article/10.1007/s12394-010-0046-y.

[17] Lerner & Mulligan, *supra* n.10, at ¶¶ 3, 41.

[18] *See* Marek Jawurek, et al., *SoK: Privacy Technologies for Smart Grids—A Survey of Options.*, 3 (2012), https://www.microsoft.com/en-us/research/wp-content/uploads/2012/11/paper.pdf.

[19] Illinois Attorney General, *Madigan: Get Smart About Smart Meters* (Mar. 25, 2016), http://www.illinoisattorneygeneral.gov/pressroom/2016_03/20160325.html (noting the capacity of smart meters to "reveal details about your life").

at work"; she rarely washes her clothes; she exercises infrequently.[20] Indeed, "[a]nyone with access to smart meter data can deduce the 'avocations, finances, occupation, general reputation, credit, health, or any other personal characteristic of the customer or the customer's household.'"[21]

Thus, because of its time granularity, smart meter data—even in aggregate form—reveals intimate details of a person's home life that would be impossible to glean from the monthly cumulative energy usage readings of analog meters.

C. Energy Disaggregation Technologies Enable More Specific Inferences About In-Home Activities.

"Energy disaggregation" uses data analytics to determine "the component appliance contributions from an aggregated electricity signal[.]"[22] It distills aggregate energy usage data into "appliance-by-appliance" data.[23] These technologies enable even more specific inferences about in-home activities from aggregate smart meter data.

Energy disaggregation technologies are well beyond the realm of "theoretic possibilit[y]." *NSMA v. Naperville ("NSMA III")*, 114 F. Supp. 3d 606, 613 (N.D. Ill. 2015). An ever-growing number of electrical utilities across the world are purchasing and implementing energy disaggregation technologies—including

---

[20] *See* Cavoukian, *supra* n.16.

[21] McNeil, *supra* n.13, at 205 (citation omitted).

[22] J. Zico Koler & Matthew J. Johnson, *REDD: A Public Data Set for Energy Disaggregation Research,* 1 (2011), https://ai2-s2-pdfs.s3.amazonaws.com/d85a/51e2978f4563ee74bf9a09d3219e03799819.pdf.

[23] Daniel A. Kelly, *Disaggregating Smart Meter Readings using Device Signatures*, 7 (Sept. 2011), https://pdfs.semanticscholar.org/a41e/097fdebc440e8babd6ed2dccc837df8c3b04.pdf.

ComEd, the largest electricity utility in Illinois, serving more than 3.7 million customers in the Chicago and Northern Illinois area.[24] One report called energy disaggregation "one of [2015's] hottest innovations in the utility data analytics space."[25]

With energy disaggregation, smart meter data can be used to not only "compile lists of household appliances"[26] and demonstrate how often each appliance is used, but also determine whether specific appliances are in good condition[27]—information that in turn could reveal household income. Disaggregation even enables use of smart meter data to pinpoint where within a home an appliance is being used.[28] Thus, as a result of disaggregation technologies, it is not only becoming increasingly easier to draw inferences about activities within the home from smart meter data, but the inferences that can be drawn are increasingly specific.

---

[24] *See* Bidgely, *Customers & Partners*, https://www.bidgely.com/customers/ (listing ComEd as a customer).

[25] Verdantix, *Funding Continues to Pour into Energy Data Disaggregation Software* (Nov. 3, 2015), http://www.verdantix.com/blog/funding-continues-to-pour-into-energy-data-disaggregation-software.

[26] Mikhail A. Lisovich, et al., *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, 13 (Jan./Feb. 2010), http://wisl.ece.cornell.edu/wicker/SWicker_lisovich.

[27] *See* Cavoukian, *supra* n.16, at 284.

[28] *See* Gerard Wynn, *Privacy concerns challenge smart grid rollout*, Reuters (June 25, 2010), http://www.reuters.com/article/energy-smart-idUSLDE65N2CI20100625 (noting that smart meter data can be used to infer whether a person is upstairs or downstairs).

II. THE FOURTH AMENDMENT PROTECTS SMART METER DATA.

A. Information Regarding the Interior of a Home Is Subject to the Utmost Fourth Amendment Protection.

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *See Kyllo*, 533 U.S. at 33 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (Harlan, J., concurring)). "At the [Fourth Amendment's] very core stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961). Indeed, the Constitution explicitly provides, "The right of the people to be secure in their . . . houses . . . shall not be violated." U.S. CONST. amend IV. Thus, while "the Fourth Amendment protects the individual's privacy in a variety of settings[,] . . . [i]n none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms[.]" *Payton v. New York*, 445 U.S. 573, 589 (1980). The home is the "sacred site" at the heart of the Fourth Amendment.[29]

Because "it is beyond dispute that the home is entitled to special protection as the center of the private lives of our people[,]" the "[s]ecurity of the home must be guarded by law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems." *Carter*, 525 U.S. at 99 (Kennedy, J., concurring). Thus, the U.S. Supreme Court has time and time again found that the

[29] Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 Cornell L. Rev. 905, 913 (2010).

Fourth Amendment stands as a bulwark against intrusions into the privacy of American homes—even in the face of technologies or tools that have threatened it.

In *Kyllo*, the Court addressed whether the warrantless use by law enforcement of a thermal imaging device "to explore details of the home that would previously have been unknowable without physical intrusion" violated the Fourth Amendment. 533 U.S. at 40. The raw thermal imaging data showed that "the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex." *Id.* at 30. The investigators inferred from this raw data that the defendant "was using halide lights to grow marijuana in his house, which indeed he was." *Id.* The government argued that warrantless collection of raw thermal imaging data was constitutional because the data did not constitute "intimate details" of the home. But the Court rejected this argument; in the home, the Court held, "*all* details are intimate details[.]" *Id.* at 37 (emphasis in original). The Court found that the raw thermal imaging data constituted intimate "information regarding the interior of the home" protected by the Fourth Amendment. *Id.* at 34 & n.2.

Kyllo also rejected the dissent's "novel proposition" that because the officers needed to make inferences based on the raw thermal imaging data collected from within the home in order to make use of it, the raw data was beyond Fourth Amendment protection. *Id.* at 36 & n.4. That the investigators made inferences based on information from the thermal imager did not "insulate[]" the unconstitutional search of the defendant's home. *Id.* at 36. According to the

majority, "[t]he issue in this case is not the police's allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house." *Id.* at 37, n.4. The warrantless collection of raw thermal imaging information was enough to violate the Fourth Amendment, regardless of whether or not the investigators conducted any post-collection analysis using the data; how the investigators were using the data was irrelevant.

In *United States v. Karo*, 468 U.S. 705, 714 (1984), the Court addressed "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." The Court held that it did. The beeper had allowed DEA agents to infer that a container of chemicals was "actually located *at a particular time in the private residence* and [was] in the possession of the person or persons[.]" *Id.* at 715 (emphasis added). The beeper revealed "a critical fact about the interior of the premises . . . that [the agents] could not have otherwise obtained without a warrant." *Id.* at 715.

In *Florida v. Jardines*, 133 S.Ct. 1409 (2013), the Court addressed whether the warrantless use of a trained narcotics dog on the front porch of the defendant's home —"a super-sensitive instrument, which [police officers] deployed to detect things inside [the home] that they could not perceive unassisted"— violated the Fourth Amendment. *See id.* at 1418 (Kagan, J., concurring). Despite prior case law concluding that warrantless canine inspections of luggage at the airport, or of an automobile during a lawful traffic stop, did not violate a person's reasonable

expectation of privacy,[30] the Court refused to permit such searches of the home. The warrantless dog sniff on the defendant's porch—used to "'explore details of the home' . . . that [the officers] would not otherwise have discovered without entering the premises"—was an invasion of the home that violated the Fourth Amendment. *Id.* at 1414–17; *id.* at 1419 (Kagan, J., concurring) (quoting *Kyllo*, 533 U.S. at 40).

B. Smart Meter Data Is Intimate Information Regarding the Interior of a Home.

As explained above, smart meters collect and record electricity usage data from directly inside the home. As in *Kyllo*, there is "no basis for saying [a smart meter reading] is not information regarding the interior of the home[.]" *Id.* at 35, n.2. Because all details of the home are intimate details protected under *Kyllo*, the analysis of whether smart meter data is entitled to Fourth Amendment protection should end here.

The district court found, however, that because "[d]ata from the City's smart meters shows only total usage and no further details[,]" there is "no reasonable expectation of privacy in that data as a matter of law[.]" *NSMA v. Naperville ("NSMA II"),* 69 F. Supp. 3d 830, 840 (N.D. Ill. 2014). First, even if it were true that aggregate smart meter data revealed "no further details" (as outlined above, it is not), under *Kyllo* it shouldn't matter. *Kyllo's* raw thermal imaging data—which revealed merely "the relative heat of various rooms in the home[,]" 533 U.S. at 35, n.2—was protected under the Fourth Amendment regardless of whether the agents

[30] The theory in these cases was that the canine inspections revealed only the presence of narcotics, a contraband item. *See United States v. Place*, 462 U.S. 696, 707 (1983); *Illinois v. Caballes*, 543 U.S. 405, 409 (2005).

needed to draw inferences from the data in order to put it to use. It was data about the inside of the home, so it was protected—raw or not. *Id.* at 36 & n.4.

Here, smart meter readings are "intimate details because they [are] details of the home, just as was the detail of how warm—or even how relatively warm—Kyllo was heating his residence." *See id.* at 38. Indeed, the aggregate data automatically collected every 15 or so minutes via smart meters is *at least as sensitive* as the raw thermal imaging data collected in *Kyllo*. The information is thus protected under the Fourth Amendment, regardless of whether or not the City conducts any post-collection analysis with the data.

Considering that smart meter data can be used to infer a far more detailed picture of the interior of a home and of the lives of its inhabitants than the grainy thermal images in *Kyllo*, smart meter data is arguably *more sensitive*. *See id.* at 52 (appendix featuring infrared image submitted as evidence in the case). But as a matter of law that does not matter. The district court's holding suggests that different types of information about the interior of a home should receive different levels of Fourth Amendment protection, but *Kyllo* explicitly rejected this proposition. The Court held that drawing "a distinction among different types of information" based on whether a homeowner truly considered the information to be "intimate"—*i.e.*, "whether the 'homeowner would even care'" if the information were revealed to or noticed by another person—would be unworkable. *Id.* at 39. Such a test could not depend on the equipment used because "there is no necessary connection between the sophistication of the surveillance equipment and the

'intimacy' of the details that it observes[.]" *Id.* at 38. And even when dealing with "relatively crude" technologies, courts must adopt rules that "take account of more sophisticated systems that are already in use or in development." *Id.* at 36. Furthermore, developing a jurisprudence outlining which aspects of home life are "intimate" and which are not would cut against the "firm" and "bright" line the Fourth Amendment places around the home. *Id.* at 39–40. American "people in their houses . . . deserve more precision." *Id.* at 39. Thus, even if aggregate smart meter data were no more intimate than raw thermal imaging data, it would nonetheless be due Fourth Amendment protection.

The district court also suggested that there is no reasonable expectation of privacy in smart meter data because certain inferences that might be drawn from the data—such as whether or not someone was likely home—could also be observed by an outsider walking past on the sidewalk. *NSMA II*, 69 F. Supp. 3d at 841. But *Kyllo* explicitly held that such comparisons—"in which outside observers might be able to perceive, *without technology*, the heat of the home"—are irrelevant for assessing whether an expectation of privacy exists in data obtained *with technology*. 533 U.S. at 35, n.2 (emphasis added). "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Id.*

Thus, like the relative heat data at issue in *Kyllo*, smart meter data collected directly from inside homes and reflecting in-home activities constitutes "intimate details" entitled to the utmost Fourth Amendment protection.

C. Americans Reasonably Expect Data About Their In-Home Activities—Including Smart Meter Data—to Remain Private.

A "normative inquiry"[31] into Americans' privacy expectation surrounding data regarding and reflecting their in-home activities confirms that Americans believe such data to be private, and that this expectation is reasonable. *See Oliver v. United States*, 466 U.S. 170, 178 (1984) (noting that one factor the Court uses to assess "the degree to which a search infringes upon individual privacy" is the "societal understanding that certain areas deserve the most scrupulous protection from government invasion"). Recent studies show, for example, that Americans express particular sensitivity about data tied to their homes. In 2016, Pew Research Center reported that 54% of American adults thought it would be "acceptable" to install surveillance cameras *in their offices* to improve workplace security and reduce theft. Only 27% of adults, however, deemed "acceptable" installation of potentially energy saving "smart thermostats" *in their homes* in return for basic behavioral data, like when they were home or moved from room to room; the

[31] In *Smith v. Maryland*, 442 U.S. 735, 741 (1979), the Court noted that a "normative inquiry" was appropriate for assessing the scope of Fourth Amendment protection in cases "where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms[.]" 442 U.S. at 740, n.5. Here, although energy utility companies have long collected monthly energy usage data and personal billing information from consumers in exchange for providing electricity, advancements in technology have quantitatively and qualitatively altered the nature of energy usage records; they can now be used to paint a detailed picture of activities within the home—the well-recognized core of Fourth Amendment protection. Thus, as explained in Section II(D), *infra*, case law regarding the expectation of privacy in monthly cumulative data from analog meters is inapposite. Rather, a normative inquiry is appropriate.

majority of adults (55%) viewed it as "not acceptable."[32] One respondent stated the reason for their answer as: "Because in your home you are not being watched or tracked and that should be your one place away from all that sensor nonsense."[33] Another put it more simply: "My home. My temperatures. My control."[34]

Studies also show that people expect privacy in the details of their day-to-day activities. In 2015, Pew reported that "[t]he majority of Americans believe it is important – often 'very important' – that they be able to maintain privacy and confidentiality in commonplace activities of their lives."[35] According to Pew's findings, 93% of adults said that being in control of *who* can get information about them was important, while 90% of adults said that controlling *what* information is collected about them was important.[36]

It should thus not be surprising that the public has been wary of smart meters, which record details from inside the home about commonplace activities of people's day-to-day lives. As Forbes reported in 2014, "[p]rivacy is probably the most

---

[32] Lee Rainie, *How Americans balance privacy concerns with sharing personal information: 5 key findings*, Pew Research Center (Jan. 14, 2016), http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/.

[33] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing—7. Scenario: Home activities, comfort and data capture*, Pew Research Center (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/scenario-home-activities-comfort-and-data-capture/.

[34] *Id.*

[35] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[36] *Id.*

sensitive issue" for consumers when it comes to smart meters.[37] The American Public Power Association, which represents more than 2,000 publicly owned electric utilities, has reported that although the number of smart meter installations is on the rise, "[o]ne of the primary challenges to full customer acceptance is concern over data privacy."[38]

In response to consumer concern over the privacy implications of smart meter data, states have begun enacting laws protecting the data collected via smart meters.[39] In 2010, for instance, the California legislature passed a law prohibiting utilities from sharing or otherwise disclosing customers' consumption data and patterns to third parties without consent; it also required utilities to maintain "reasonable security procedures," including encryption, for customers' electricity or gas usage data. *See* Cal. Pub. Util. Code §§ 8380–8381 (codifying S.B. 1476). A 2013 law extended those same protections to smart meter data in the hands of Internet

---

[37] Federico Guerrini, *Smart Meters: Between Economic Benefits And Privacy Concerns*, Forbes (June 1, 2014), http://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/#83aae4d51a93.

[38] Paul Zummo, *Smart Grid Data Privacy Concerns: An Overview of Recommended Guidelines*, American Public Power Association (Aug. 2014), http://www.publicpower.org/files/images/BookStore/APPA_Privacy_Concerns_guidelines.pdf.pdf.

[39] *See, e.g.*, Okla. Stat. Ann. tit. 17, § 710.4(A), (B) (placing limits on disclosure of customer information to third parties and requiring that disclosure of aggregate usage data contain a sufficient number of similarly situated customers so that daily usage routines or habits of individual customers cannot reasonably be deduced); 4 N.C. Admin. Code 11.R8-60.1 (requiring utilities to submit, for all smart grid technologies, a plan describing, *inter alia*, how customers will authorize the utilities to release their information to third parties); Me. Rev. Stat. tit. 35-A, § 3143 (permitting Maine's public utilities commission to adopt rules regarding the implementation of smart grid functions in the state, including rules regarding cybersecurity and protection of consumer privacy).

Service Providers ("ISPs"), financial institutions, and other businesses. *See* Cal. Civ. Code § 1798.98. In addition, in 2011, the California Public Utilities Commission adopted rules prohibiting the use or disclosure of electrical or gas usage information that could be used to identify an individual, family, household for any "secondary purpose" without obtaining the prior written authorization for each secondary purpose.[40] It also prohibited utilities from disclosing to any third party more information than "reasonably necessary" to carry out either the utility's "primary purpose" with the data or the specific secondary purpose authorized by the customer.[41]

Such efforts on the part of state legislatures and utility commissions to protect the privacy of smart meter data support that Americans' expectation of privacy in this data is reasonable. Indeed, the existence of statutory protection for certain kinds of information helps inform whether society has determined that a particular expectation of privacy is reasonable. *See, e.g., United States v. Maynard*, 615 F.3d 544, 564 (D.C. Cir. 2010) ("[S]tate laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable."); *Doe v. Broderick*, 225 F.3d 440, 450 (4th Cir. 2000) (federal statutory protection "is relevant to the determination of whether there is a 'societal understanding'" of a legitimate expectation of privacy in medical records).

---

[40] Cal. Pub. Util. Comm'n, *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company*, 75 (July 29, 2011), https://cdt.org/files/pdfs/PUC%20Smart%20Grid%20Final.pdf.

[41] *Id.* at 68.

D. Case Law Regarding the Expectation of Privacy in Monthly, Cumulative Analog Meter Data Is Inapposite.

The lower court relied on cases involving monthly cumulative electricity usage data generated via analog meters to conclude that people have no reasonable expectation of privacy in any aggregate electricity usage records as a matter of law—regardless of whether that data was collected via a smart meter or an analog meter. *See NSMA v. Naperville* ("*NSMA I")*, No. 11 C 9299, 2013 WL 1196580, at *12 (N.D. Ill. 2013) (noting an "already-surrendered privacy interest in the aggregate measurement of their electricity usage").

These cases are inapposite; they involved single monthly cumulative energy readings and zero time granularity. *See United States v. McIntyre*, 646 F.3d 1107, 1110 (8th Cir. 2011) (involving a single sheet of electrical usage data containing three years' worth of monthly cumulative readings); *United States v. Hamilton*, 434 F. Supp. 2d 974, 978 (D. Or. 2006) (involving eleven-months of subscriber information and cumulative monthly power consumption readings for the defendant's home, along with that of previous residents and four neighbors); *United States v. Porco*, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) (involving average monthly electrical use readings, as used to generate a monthly bill).

As explained above, because of its time granularity, smart meter data is both qualitatively and quantitatively different than analog meter data. When it comes to new technologies, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *See City of Ontario, Cal. v. Quon*, 560 U.S. 746,

759 (2010). The district court thus erred in "mechanical[ly]" applying pre-digital rules designed for analog devices—devices with but a tiny fraction of the capability of modern smart meters—rather than carefully considering Americans' expectation of privacy in the sensitive information generated by these new technologies. *See Riley v. California*, 134 S. Ct. 2473, 2484 (2014).

E. Americans' Expectation of Privacy in Smart Meter Data Is Objectively Reasonable Even Though An Energy Utility May Have Access to the Data.

The district court also erroneously relied on *Smith v. Maryland* to conclude that Americans have no reasonable expectation of privacy in smart meter data shared with utility companies. *Smith* addressed whether the government needed a warrant to gain access to dialed phone numbers held by a private phone company. 442 U.S. at 736–38. Because this case involves a municipal utility company—a governmental entity—obtaining data directly from citizens, the so-called "third party doctrine" outlined in *Smith* is inapplicable.

Even if *Smith* were applicable, its reasoning applies only to data "voluntarily" conveyed to a third party, and smart meter data is in no way voluntarily conveyed to energy utilities. Even if it were, the Supreme Court has made clear that the Fourth Amendment protects sensitive personal information, such as smart meter data, even when it is known that third parties have access to it.

i. Consumers Do Not "Voluntarily Convey" Smart Meter Data To Their Energy Utility.

Smith held that individuals have no reasonable expectation of privacy in the numbers dialed into a telephone system because they are business records

"voluntarily conveyed" to the phone company. 442 U.S. at 744. Applying *Smith*, the district court held that the NSMA plaintiffs had no reasonable expectation of privacy in smart meter data because they "knowingly conveyed the aggregate measurements of their electricity usage directly to the party from which they wish to keep it a secret." *NSMA I*, 2013 WL 1196580, at *12.

Unlike when someone affirmatively dials a specific telephone number, however, consumers do not *voluntarily* transmit detailed energy usage data to utility companies every 15 or so minutes. In many cities, smart meters are either mandatory or consumers are required to pay monthly fees to opt out.[42] Indeed, smart meters are an increasingly "pervasive and insistent part of daily life[.]" *See Riley*, 134 S. Ct. at 2484. Consumers thus often have little choice but to share smart meter data with their utility companies—that is, if they wish to have electricity in their homes. *Cf. State v. Earls*, 70 A.3d 630, 587 (N.J. 2013) (holding that the third party doctrine should not apply where "cell-phone users have no choice but to reveal certain information to their cellular provider").

Furthermore, unlike in *Smith*, a consumer does not *affirmatively*—let alone *knowingly* in many cases[43]—generate and transmit energy usage data to their

[42] In California, residents are charged a one-time fee of up to $75 for analog meters in addition to 36 monthly charges of up to $10. *See, e.g.*, PG&E, *Learn about your meter choices*, https://www.pge.com/en_US/residential/save-energy-money/analyze-your-usage/your-usage/view-and-share-your-data-with-smartmeter/smartmeter-updates/smart-meter-opt-out-program.page.

[43] According to a 2011 study, "70 percent of consumers reported being aware of 'smart grid technology' but only 'somewhat understand how it works.'" Andrew Nusca, *Majority of Americans don't understand smart grid, study says*, ZDNet (Mar.

electrical utility. The information is collected automatically—without any consumer involvement—via a continually running and often out-of-sight device, without any of the "intent, awareness, or affirmative conduct" on the part of the consumer that was at issue in *Smith*.[44] Such *passive*, *unknowing* generation of data cannot amount to a "voluntary conveyance" under the third-party doctrine. Indeed, the premise that an individual has no reasonable expectation of privacy in any information disclosed to third parties "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

ii. The Fourth Amendment Protects Sensitive Information Even if People Know a Third Party May Access It.

Even if users somehow "voluntarily" conveyed their smart meter data to their electrical utility, *Smith* did not create a blanket rule that all information shared with a third party is denied Fourth Amendment protection. The Supreme Court has made clear that the fact that sensitive information is held by a third party does not automatically defeat an individual's expectation of privacy in the information.

29, 2011), http://www.zdnet.com/article/majority-of-americans-dont-understand-smart-grid-study-says/.

[44] *See In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1026, 1029, 1033 (N.D. Cal. 2015) (holding that "the generation of historical CSLI [cell site location information] via continually running apps or routine pinging is not a voluntary conveyance by the cell phone user" and thus "does not defeat a cell phone user's reasonable expectation of privacy in the historical CSLI associated with her cell phone"); *see also United States v. Davis*, 785 F.3d 498, 534 (11th Cir. 2015) (Martin, J., dissenting); *Tracey v. State*, 152 So.3d 504, 525–26 (Fla. 2014).

In *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001), the Court held that hospital patients have a reasonable expectation of privacy in diagnostic test results held by the hospital—specifically, that they could reasonably expect their test results would not be shared with nonmedical personnel without consent. In *Bond v. United States*, 529 U.S. 334, 338–39 (2000), the Court held that a passenger retained an expectation of privacy in luggage placed in a bus overhead bin, despite the possibility of external inspection by others. In *Stoner v. California*, 376 U.S. 483, 489–90 (1964), the Court held that hotel guests were entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms. Relevant here, the Court equated a hotel room to the home of a tenant in terms of the level of constitutional protection against unwarranted searches and seizures, noting that "[t]hat protection would disappear if it were left to depend upon the unfettered discretion of an employee of the hotel." *Id.* at 490. And in *Ex parte Jackson*, 96 U.S. 727, 733 (1877) the Court held that sealed letters could not be opened and examined without a warrant even though they were in the custody of the U.S. Postal Service. *See also United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) (holding that there is a reasonable expectation of privacy in the contents of emails, despite being sent via an Internet service provider's servers).

Here, the compulsory conveyance of data reflecting intimate details of in-home activities does not—and cannot—extinguish the strong expectation of privacy that Americans reasonably have in smart meter data. Indeed, the Fourth

Amendment protection afforded to the home "would be of little practical value" if Americans were said to have no expectation of privacy in smart meter data. *See Jardines*, 133 S.Ct. at 1414. Government officials would be free to seek access to a person's smart meter profile at any time to understand intimate details about their daily patterns and home life. The Fourth Amendment's strong protection for the intimate details of the home condemns this result.

CONCLUSION

For the foregoing reasons, this Court should reverse the district court's holding.

Dated: February 28, 2017

By: */s/ David Greene*

David Greene (*Counsel of Record*)
Jamie L. Williams
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
davidg@eff.org

Caroline Wilson Palow
Scarlet Kim
PRIVACY INTERNATIONAL
62 Britton Street
London EC1M 5UY
United Kingdom
+44 (0) 20 3422 4321
caroline@privacyinternational.org

Counsel for *Amici Curiae*
Electronic Frontier Foundation and
Privacy International

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and Circuit Rule 29 because this brief contains 6,966 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Word 2011 in 12-point Century Schoolbook.

Dated: February 28, 2017

By: */s/ David Greene*
David Greene

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the appellate CM/ECF system on February 28, 2017.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: February 28, 2017

By: */s/ David Greene*
David Greene

Counsel for Amici Curiae