UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 93 | Number 4 Article 5

5-1-2015

The Home Out of Context: The Post-Riley Fourth Amendment and Law Enforcement Collection of Smart Meter Data

Natasha H. Duarte

The Home Out of Context: The Post-*Riley* Fourth Amendment and Law Enforcement Collection of Smart Meter Data*

INTRODUCTION

Smart meters[1] know when you're sleeping. They know when you're awake. They might even know whether you're in the shower or watching TV.[2] Utility companies are steadily installing these smart meters on consumers' homes.[3] Unlike traditional energy meters, which show a household's aggregated electricity use each month, smart meters collect fine-grained, minute-by-minute data about electricity use and transmit it back to the utility at regular intervals.[4] This data, when collected over time and analyzed, can reveal the activities and behavioral patterns of a household.[5] Utility records have long been of interest in law enforcement investigations,[6] and the

1. Smart meters, also referred to as Advanced Metering Infrastructure ("AMI"), are electronic utility meters that enable two-way communication between utilities and consumers. *See* Recovery Act Smart Grid Programs, U.S. Dep't of Energy, *Advanced Metering Infrastructure and Customer Systems*, SMARTGRID.GOV, https://www.smartgrid.gov/recovery_act/deployment_status/ami_and_customer_systems (last visited Apr. 10, 2015). These meters "collect highly granular data on individual electricity consumption and allow users to monitor and remotely control their electrical use . . . ." Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 200 (2011).

2. *See* 2 NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBERSECURITY 27 (2010) [hereinafter NIST], *available at* http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (concluding that, when analyzed, smart meter data can reveal information about people's lifestyles and appliance use); Jordan Robertson, *Your Outlet Knows: How Smart Meters Reveal Behavior at Home, What We Watch on TV*, BLOOMBERG (June 10, 2014), http://www.bloomberg.com/news/2014-06-10/your-outlet-knows-how-smart-meters-can-reveal-behavior-at-home-what-we-watch-on-tv.html (reporting on a German study where researchers were able to ascertain the specific television programs people were watching based on data collected by smart meters).

3. *See, e.g.*, ENERGY INFO. ADMIN., U.S. DEP'T OF ENERGY, U.S. SMART GRID CASE STUDIES 1 (2011), *available at* https://www.smartgrid.gov/sites/default/files/doc/files/smartggrid%5B1%5D.pdf ("A recent report . . . predicts that U.S. smart meter installations will exceed 80 million by 2015, up from 2 million in 2007."). *But see Smart Electric Meters, Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts 2014,* NAVIGANT RES., http://www.navigantresearch.com/research/smart-meters (last visited Apr. 10, 2015) ("The smart electric meter market has shifted emphasis to projects in Europe and Asia Pacific while the once hot U.S. market has leveled off, as federal funding for projects has been nearly exhausted.").

4. *See Smart Meter Deployments Continue to Rise*, EIA (Nov. 1, 2012), http://www.eia.gov/todayinenergy/detail.cfm?id=8590.

5. *See* NIST, *supra* note 2, at 27; Robertson, *supra* note 2.

6. BRANDON J. MURRILL ET AL., CONG. RESEARCH SERV., R42338, SMART METER DATA: PRIVACY AND CYBERSECURITY 5 (2012), *available at* http://fas.org/sgp/crs/

detailed information contained in smart meter data can provide police with infinitely more insight into people's homes.[7]

Traditionally, law enforcement would need a warrant to gain access to one's home.[8] However, smart meters take information about the activities that occur inside the home and put it in the hands of a third party—the utility company.[9] Under the Third-Party Doctrine, that information loses Fourth Amendment protection and becomes subject to warrantless collection.[10] This counter-intuitive result is produced by a line of Fourth Amendment cases that have conceptualized privacy as binary: personal information is either private or has been shared with a third party for any reason, making it public.[11]

misc/R42338.pdf ("In the past, law enforcement agents have examined monthly electricity usage data from traditional meters in investigations of people they suspected of illegally growing marijuana."). For legal background on law enforcement's use of utility records, see generally United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108 (9th Cir. 2012); United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011); Idaho v. Kluss, 867 P.2d 247 (Idaho Ct. App. 1993); New Jersey v. Domicz, 871 A.2d 744 (N.J. Super. 2005).

7. MURRILL ET AL., *supra* note 6, at 1 ("As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations."); Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid 4, Order Instituting Rulemaking to Consider Smart Grid Tech., RM 08-12-009 (Pub. Util. Comm'n of the State of Cal. Dec. 18, 2008), *available at* https://www.eff.org/files/cdteffjointcomment030910.pdf [hereinafter CDT & EFF Joint Comments].

8. Kyllo v. United States, 533 U.S. 27, 31 (2001) ("The Fourth Amendment provides that 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.' . . . With few exceptions, the question [of] whether a warrantless search of a home is reasonable and hence constitutional must be answered no." (alteration in original)).

9. *See supra* note 4 and accompanying text.

10. *See McIntyre*, 646 F.3d at 1111–12 (applying Smith v. Maryland, 442 U.S. 735 (1979), in which the Court found no expectation of privacy in phone records "voluntarily conveyed" to a telephone company, and holding that the same was true of utility records "voluntarily conveyed" to a utility company). For an explanation of the Third-Party Doctrine, see *infra* text accompanying notes 53–64.

11. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979). (Marshall, J., dissenting) (criticizing the Court for treating privacy as a "discrete commodity, possessed absolutely or not at all"); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) (arguing that courts, in "treating exposure to a limited audience as identical to exposure to the world," have failed "to recognize degrees of privacy in the Fourth Amendment context"); Helen Nissenbaum, *Privacy As Contextual Integrity*, 79 WASH. L. REV. 119, 136–37 (2004) (arguing that current legal approaches express "a right to privacy in terms of dichotomies—sensitive and non-sensitive, private and public, government and private . . . . That which falls within any one of the appropriate halves warrants privacy consideration; for the rest, anything goes"). Daniel Solove has referred to this concept as "privacy as secrecy"—if information is no longer totally secret, it is public. Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1107 (2002) ("In a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is

Since the adoption of the "reasonable expectation of privacy" test in *Katz v. United States*,[12] courts have relied on public/private dichotomies as substitutes for genuine inquiries into society's expectations of privacy.[13] The Third-Party Doctrine epitomizes this binary approach, holding that information disclosed to a third party under any circumstances is public.[14] The doctrine has been invoked to remove Fourth Amendment protection from financial records,[15] phone records,[16] cell site location data,[17] email records,[18] and Internet browsing data.[19] Much of our personal information—whom we call or email, what we buy, what we read, where we travel—is contained in electronic records, and many of these records are stored on third-party servers.[20] By removing constitutional privacy protections from

divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private.").

12. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

13. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 113–14 (2010); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 7 (2007); Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 826–27 (2010) (citing Alan Freeman & Elizabeth Mensch, *The Public-Private Distinction in American Law and Life*, 36 BUFF. L. REV. 237, 247–50 (1987)); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 657–59 (2013); Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 377–80 (2013).

14. *See* Colb, *supra* note 11, at 122.

15. United States v. Miller, 425 U.S. 435, 440 (1976).

16. *Smith*, 442 U.S. at 745–46.

17. *See generally* United States. v. Guerrero, 768 F.3d 351 (5th Cir. 2014) (holding government's violation of the Stored Communications Act did not require suppression of defendant's historical cell cite location data); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that the Fourth Amendment probable cause standard is not applicable to historical cell site information); *In re* Application of U.S.A. for an Order Pursuant to 18 U.S.C. §§ 2703(c) and 2703(d) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS and Verizon Wireless to Disclose Cell Tower Log Information, No. M-30, 2014 WL 4388397 (S.D.N.Y. May 30, 2014) (holding the Fourth Amendment did not preclude the government from requiring providers to disclose historical cell site data); United States v. Caraballo, 963 F. Supp. 2d 341 (D. Vt. 2013) (holding that defendant had no reasonable expectation of privacy in his real time cell phone location information); United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (finding that defendants did not have a legitimate expectation of privacy in historical cell site location records); United States v. Gordon, No. 09-153-02 (RMV), 2012 WL 8499876 (D.D.C. Feb. 6, 2012) (finding that no reasonable expectation of privacy exists for cell site location data shared with third parties).

18. United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2007).

19. *Id.*

20. *See* Spencer, *supra* note 13, at 390–91 ("[T]he Internet service providers on whom we rely for essential connectivity record the websites we visit, the files we download, and the people whom we email or message. Everyday transactions, both online and in real space, convey a plethora of data to third parties.").

this vast swath of data, the Third-Party Doctrine has swallowed the Fourth Amendment. Scholars have argued that the Third-Party Doctrine's blunt approach does not fit the reality of digital data.[21] Some scholars have advanced a "contextual approach" to Fourth Amendment privacy—one that looks to social norms to determine whether a particular disclosure is "expected" under the circumstances.[22]

With its recent decision in *Riley v. California*,[23] the Supreme Court has taken an encouraging step toward a more contextual approach to digital privacy.[24] In *Riley*, a unanimous Court refused to extend the search-incident-to-arrest warrant exception to the contents of an arrestee's cell phone.[25] Although *Riley* did not deal directly with the Third-Party Doctrine,[26] it weakened the doctrine's assumptions in at least two ways. First, the *Riley* Court acknowledged that digital data, stored and aggregated in large quantities, can reveal a detailed picture of an individual's private life, imbuing each individual piece of data with an informational value that it might not have had standing alone.[27] In fact, the Court compared the contents of a cell phone to the contents of one's home.[28] Second, and more importantly, the Court rejected the assumption that expectations of privacy are binary when it held that an arrestee could forfeit Fourth Amendment protection in a cigarette pack but not a cell phone, even if both were stored in his pocket.[29]

21. *See, e.g.*, *id.* at 376 (describing the ways in which "the binary conception of privacy cannot address the third-party privacy problem in the emerging surveillance society"); Solove, *supra* note 11, at 1151–52 ("The Court's jurisprudence in these [Third-Party Doctrine] cases conceptualizes privacy as a form of total secrecy; however, this conception is ill-suited for the circumstances involved in these cases. . . . Life in the modern Information Age often involves exchanging information with third parties . . . . Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world.").

22. Nissenbaum, *supra* note 11, at 120; Selbst, *supra* note 13, at 643–44; Solove, *supra* note 11, at 1091–92; Spencer, *supra* note 13, at 373.

23. 134 S. Ct. 2473 (2014).

24. *See id.* at 2478.

25. *Id.* at 2485.

26. *Id.* at 2489 n.1 ("[T]hese cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

27. *See id.* at 2489.

28. *Id.* at 2491. ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house . . . .").

29. *See id.* at 2488 ("The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely . . . . The United States asserts that a search of all data stored on a cell phone is 'materially

In the Court's view, the mere fact that we can now carry vast amounts of personal information in our pockets does not mean we do not expect some privacy in that data.[30] Third-Party Doctrine critics argue that the same is true of information held by third parties—it subverts society's expectations to hold that information stored on a hard drive is private while information stored in the cloud is public.[31] This Recent Development argues that when this more contextual approach is applied to the warrantless collection of smart meter data—information about activities that occur inside the home but collected by a third-party provider—the Third-Party Doctrine becomes irreconcilable with the Fourth Amendment principles articulated in *Riley*.

This Recent Development proceeds in three parts. Part I discusses the development of the Fourth Amendment expectation of privacy doctrine, focusing on how the doctrine has evolved in the face of technology. Part II discusses two categories of Fourth Amendment interpretation: one that treats information privacy as a binary public/private concept and another that treats expectations of privacy as contextual. Part II argues that *Riley*'s approach to digital privacy falls toward the latter category by subverting expectations and attempts to put privacy back in context by grappling with the realities of how we interact with technology and the expectations we have for those interactions. Part II also notes that lower courts discussing *Riley* have suggested that the Supreme Court might overturn the Third-Party Doctrine if confronted with a set of facts that was *Riley*-esque but where police obtained the data from a third party instead of directly from an individual. Part III argues that those facts can be found in the case of smart meters. By putting highly personal information—one's activities inside the home—in the hands of a third party, the smart grid models the perverse effects of the Third-Party Doctrine in the digital age.

indistinguishable' from searches of [physical items such as cigarette packs]. . . . That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.").

30. *See infra* text accompanying notes 78–92.

31. *See, e.g.*, Colb, *supra* note 11, at 155 ("The Court, however, makes the mistake of treating situations in which only a limited exposure has occurred as though there had been this kind of total, irreparable exposure. . . . The idea is flawed because it ignores norms about keeping confidences. . . . We do not expect, nor should we expect, that the strangers with whom we deal will broadcast our secrets generally.").

I. THE PRE-*RILEY* FOURTH AMENDMENT

A. The Court's Binary Approaches to Privacy

The binary approaches to the Fourth Amendment are dichotomies that courts draw, essentially creating shortcuts to determine whether a constitutionally protected privacy interest exists. The first such dichotomy was whether the government had invaded a "constitutionally protected area."[32] Before the Court introduced the "reasonable expectation of privacy" test in *Katz v. United States*,[33] the Fourth Amendment only applied to the "protected areas" enumerated in the Fourth Amendment: "Persons [e.g., bodies], houses, papers, and effects [e.g., cars]."[34] Searches typically required police to physically enter a person's home.[35] In *Olmstead v. United States*[36] and *Goldman v. United States*,[37] the Court found that tapping or otherwise eavesdropping on a person's phone call was not a Fourth Amendment search because it did not require penetration of the four walls of the home or office.[38] These early cases reflected the narrow view that the ability to obtain information without entering into a "protected area" excluded that information from Fourth Amendment protection. For Fourth Amendment purposes, information was either obtainable only in a protected area and therefore private, or the information was public.

In 1967, the Supreme Court redefined the contours of the Fourth Amendment when it decided *Katz*.[39] The Court held that FBI agents had conducted an unconstitutional warrantless search when they attached an electronic recording device to the exterior of a public phone booth and recorded Katz's conversations.[40] Rejecting the appeals court's reasoning that there was no search because the device

32. *See* Berger v. New York, 388 U.S. 41, 57, 59 (1967) ("It is true that this Court has occasionally described its conclusions in terms of 'constitutionally protected areas' . . . but we have never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem."); Katz v. United States, 389 U.S. 347, 351 n.9 (1967) (citing Silverman v. United States, 365 U.S. 505, 512 (1961)); Lopez v. United States, 373 U.S. 427, 438 (1963).

33. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

34. *See* U.S. CONST. amend. IV; *supra* note 32 and accompanying text.

35. *Katz*, 389 U.S. at 352–53 ("It is true that the absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry . . . for that Amendment was thought to limit only searches and seizures of tangible property." (citing Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928))).

36. 277 U.S. 438 (1928).

37. 316 U.S. 129 (1942).

38. 316 U.S. at 135–36; 277 U.S. at 466.

39. *Katz*, 389 U.S. at 351–53.

40. *Id.*

did not penetrate the wall of the phone booth, Justice Potter Stewart declared that "the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[41] The *Katz* Court still seemed to demand some level of secrecy,[42] but it rejected the idea that "constitutionally protected areas" could provide a "talismanic solution" to Fourth Amendment questions.[43]

When the Supreme Court introduced the "expectation of privacy" doctrine in *Katz*, it indicated that, to some extent, privacy would turn on social norms.[44] A phone booth might be more exposed than one's home, and a phone booth user may even know that his call could be intercepted, but the Court acknowledged a societal expectation that the content of one's conversation would not flow beyond the parties to the conversation.[45] However, even as it introduced this new doctrine, *Katz* maintained a binary conceptualization of privacy that relied on the secrecy of information.[46] This secrecy model has become increasingly problematic in the digital age.[47] As new technology has made it easier for law enforcement to collect formerly obscured information, courts

41. *Id.* at 351–52.

42. *Id.* at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Solove, *supra* note 11, at 1107 ("[T]he Court's Fourth Amendment jurisprudence adheres to the notion that matters that are no longer completely secret can no longer be private." (citing *Katz*, 389 U.S. at 351)).

43. *Katz*, 389 U.S. at 351 n.9.

44. Courts adopted Justice Harlan's interpretation of *Katz*, that the threshold question of whether a search occurred is whether a person "exhibited an actual (subjective) expectation of privacy" and whether that expectation was "one that society is prepared to recognize as 'reasonable.' " *Id.* at 361 (Harlan, J., concurring); *see* Colb, *supra* note 11, at 123 ("[A]n honest inquiry into whether police have acted in a manner that exposes what would have remained hidden absent the transgression of a legal or social norm . . . would adhere to the doctrinal foundations of privacy as articulated in Katz."); *see also* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) ("[W]here an individual's subjective expectation [of privacy] had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms . . . [i]n determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.").

45. *Katz*, 389 U.S. at 352 ("But what [Katz] sought to exclude when he entered the booth . . . was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. . . . [A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

46. *See* Solove, *supra* note 11, at 1107 (citing *Katz*, 389 U.S. at 351).

47. *See id.*

have envisioned privacy as a "discrete commodity" that is wholly lost once information is exposed.[48] In *United States v. Knotts*,[49] the Court held that it was not a "search" to place a beeper in a suspect's car and monitor his location using the signal, finding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[50] Instead of evaluating whether society would expect a person's every move to be followed, the Court focused on the fact that the movements occurred in public and were therefore vulnerable to collection.[51] By limiting Fourth Amendment protection to secret information, the Court has traded one binary for another.[52]

The Third-Party Doctrine is an extreme expression of this binary approach. The doctrine usually arises when law enforcement obtains information without a warrant and uses it as evidence in a criminal prosecution or to obtain a warrant.[53] Under the doctrine, if information is exposed to any third party for any reason, it is no longer private and can be obtained without a warrant.[54] The doctrine first arose in *United States v. Miller*,[55] but its widespread adoption resulted from lower-court interpretations of *Smith v Maryland*.[56] In that case, the Court held that no search occurred when law enforcement used a pen register device to obtain from the telephone company a record of the numbers dialed by an individual.[57] Justice Blackburn, writing for the Court, found that Smith had no reasonable expectation of privacy in the phone numbers he dialed, since

48. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting); *see* California v. Greenwood, 486 U.S. 35, 39–41 (1988); California v. Ciraolo, 476 U.S. 207, 212–14 (1986); United States v. Knotts, 460 U.S. 276, 281–82 (1983).

49. 460 U.S. 276 (1983).

50. *Id.* at 281.

51. Almost thirty years later, the Court considered similar facts in *United States v. Jones* but relied on the traditional trespass theory of the Fourth Amendment to find that an expectation of privacy was violated when police physically installed a GPS device on a suspect's vehicle. United States v. Jones, 132 S. Ct. 945, 950 (2012).

52. Solove, *supra* note 11, at 1107 (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)).

53. *See generally Smith*, 442 U.S. 735 (reviewing a case where the telephone company installed a pen register without a warrant to record the numbers dialed from a phone); United States. v. Guerrero, 768 F.3d 351 (5th Cir. 2014) (involving historical cell site location data that was obtained without a warrant); United States v. Forrester, 512 F.3d 500 (9th Cir. 2007) (considering a case where the government used computer surveillance techniques without a warrant).

54. *See Forrester*, 512 F.3d at 509–10.

55. 425 U.S. 435, 440–42 (1976) (holding that there was no reasonable expectation of privacy in financial documents "voluntarily conveyed" to a bank).

56. 442 U.S. 735 (1979).

57. *Id.* at 745–46.

telephone users "typically know that they must convey numerical information to the company" for "legitimate business purposes."[58] The Court in 1979 could not have foreseen its impact on privacy in the digital age, but the doctrine endures nonetheless.[59]

Now that most of our data is stored on third-party servers, the Third-Party Doctrine has effectively removed vast amounts of digital data—much of which includes personal information—from Fourth Amendment protection. Information deemed open to warrantless collection includes location data transmitted through cell phone signals,[60] IP addresses and other information provided to an Internet Service Provider,[61] and even files downloaded using peer-to-peer file sharing software.[62] As Part III will discuss, multiple federal courts have found energy usage data to be subject to warrantless collection from utility companies.[63] In many ways, the Third-Party Doctrine represents a return to outmoded ideas that the Fourth Amendment only protects certain inherently private spaces. If the doctrine were taken to its logical extreme, data stored on one's phone would be protected while the same data stored on a cloud server would be unprotected.[64] The doctrine betrays *Katz* by making this first-

58. *Id.* at 743.

59. Smith v. Obama, 24 F. Supp. 3d 1005, 1009 (D. Idaho 2014) ("*Smith* [*v. Maryland*] could never have anticipated the ubiquity of cell-phones and the fact that 'people in 2013 have an entirely different relationship with phones than they did thirty-four years ago.' " (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013))).

60. *See* United States. v. Guerrero, 768 F.3d 351, 359 (5th Cir. 2014); *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013); *In re* Application of United States for an Order Pursuant to 18 U.S.C. §§ 2703(C) and 2703(D) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS and Verizon Wireless to Disclose Cell Tower Log Information, No. M-50, 2014 WL 4388397, at *5 (S.D.N.Y. May 30, 2014); United States v. Caraballo, 963 F. Supp.2d 341, 363 (D. Vt. 2013); United States v. Graham, 846 F. Supp. 2d 384, 390 (D. Md. 2012); United States v. Gordon, No. 09-153-02(RMU), 2012 WL 8499876, at *1 (D.D.C. Feb. 6, 2012).

61. *See* United States v. Stanley, 753 F.3d 114 (3d Cir. 2014); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *1 (D. Ariz. 2013); *In re* Application of United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 114 (E.D. Va. 2011).

62. *See* United States v. Dennis, 3:13-cr-10-TCB, 2014 WL 1908734, at *1 (N.D. Ga. May 12, 2014); United States v. Thomas, 5:12-cr-37, 2013 WL 6000484, at *19–20 (D. Vt. Nov. 8, 2013).

63. *See* United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1111 (9th Cir. 2012); United States v. McIntyre, 646 F.3d 1107, 1111 (8th Cir. 2011); Naperville Smart Meter Awareness v. Naperville, No. 11 C 9299, 2013 WL 1196580, at *14 (N.D. Ill. Mar. 22, 2013); State v. Kluss, 867 P.2d 247, 247 (Idaho App. 1993); *see also infra* Part III (providing a more in depth discussion of the warrantless collection of energy usage data by utilities).

64. In the Supreme Court's *Riley* opinion, Chief Justice Roberts noted that it "makes little difference" to the user (and that in fact the user may not even know) whether

party/third-party dichotomy a "talismanic solution" to Fourth Amendment questions.

B. Contextual Approaches to Privacy

Despite this persistent trend, the Court has occasionally recognized the contextual nature of privacy, acknowledging that information can be vulnerable to collection without losing its protection wholesale.[65] The contextual approach to privacy was first introduced by Helen Nissenbaum as the "contextual integrity" theory of privacy,[66] which has since been adapted as a Fourth Amendment model by other scholars.[67] According to Nissenbaum, privacy requires "respect for the appropriate flow of information about identifiable persons within particular social contexts."[68] Different contexts, such as healthcare, home life, and finance, are governed by different information norms. These norms are determined based on the particular "actors" (the subjects, receivers, and senders of information), informational "attributes" (the type of record, e.g., a medical record), and "transmission principles" at play (e.g., whether the record was disclosed for a specific reason or use or whether there was a confidential relationship between the parties).[69] Privacy is violated when these norms are broken.[70]

In *United States v. Jones*,[71] the Court acknowledged that information once viewed as "public"—individuals' movements from place to place on public thoroughfares—might implicate privacy interests when collected over a long period of time.[72] However, the *Jones* majority resorted to the binary "trespass" theory of the Fourth Amendment to ultimately decide the case.[73] In *Kyllo v. United States*,[74] the Court refused to apply such a "mechanical interpretation of the Fourth Amendment" as to find that the use of thermal imaging was not a search because it only detected heat radiating from a home's external surface.[75] Instead, the Court found the use of

information found on a cell phone is stored on the phone itself or in the cloud. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

65. *See infra* text accompanying notes 67–72.
66. Nissenbaum, *supra* note 11, at 136–37.
67. *See* Selbst, *supra* note 13, at 643–44.
68. *Id.* at 650 (citing NISSENBAUM, *supra* note 13, at 127).
69. *Id.* at 651.
70. Nissenbaum, supra note 11, at 138.
71. 132 S. Ct. 945 (2012).
72. *Id.* at 955 (Sotomayor, J., concurring).
73. *Id.* at 950 (majority opinion).
74. 533 U.S. 27 (2001).
75. *Id.* at 28.

technology to obtain information about the interior of the home analogous to physically intruding into the home.[76] Unfortunately, *Kyllo* also stopped short of a truly contextual approach to privacy. Justice Scalia's majority opinion emphasized the use of technology "not in general public use" to obtain information "regarding the interior of the home" not otherwise obtainable without physical intrusion.[77] *Kyllo* thus left unanswered the question of whether a technology in general use, such as a smart meter, could reveal personal information in a context that is contrary to society's expectations. As Part II will discuss, *Riley* went a step further toward contextualizing privacy.

II. THE *RILEY* COURT'S APPROACH TO DIGITAL DATA

In *Riley*, the Supreme Court considered whether cell phone data fell under the search-incident-to-lawful-arrest warrant exception, which allows officers to search an arrestee's person, including items found in his pockets, such as a cigarette pack.[78] A unanimous Court found that a warrant was required to search a cell phone because "digital information on a cell phone . . . implicates substantially greater individual privacy interests than a brief physical search."[79] Chief Justice Roberts, writing for the Court, compared a cell phone to a person's house[80] in its capacity to hold different types of data in large quantities and reveal "[t]he sum of an individual's private life."[81] Moreover, the Court did not find that the search was justified based on the "arrestee's reduced privacy interests upon being taken into police custody."[82] The Court found the search to be more than a "minor additional intrusion[]" into the arrestee's privacy.[83] Roberts wrote that "[t]he fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely."[84] The Court declined to categorically subject to unwarranted search all of an arrestee's information simply because he could carry it in a device in his pocket.[85] Thus, the *Riley* Court rejected a binary application of the Fourth Amendment and

76. *Id.*
77. *Id.* at 34.
78. Riley v. California, 134 S. Ct. 2473, 2484 (2014).
79. *Id.* at 2478.
80. *Id.* at 2491.
81. *Id.* at 2489.
82. *Id.* at 2488.
83. *Id.*
84. *Id.*
85. *Id.* at 2488–89.

acknowledged that the nature of digital data and the context of disclosure bear on society's expectations of privacy.

The privacy interests in *Riley* turned on the ability of digital data, when stored in large quantities, to reconstruct a person's life.[86] Chief Justice Roberts's opinion focused on the "quantitative" and "qualitative" differences between digital data stored on a cell phone and physical objects such as a cigarette pack.[87] Roberts wrote that cell phones combine "immense storage capacity" with "the ability to store many different types of information," resulting in data "that reveal much more in combination than any isolated record," and allowing "even just one type of information to convey far more than previously possible."[88] Citing Justice Sotomayor's concurrence in *United States v. Jones*,[89] the Chief Justice concluded that "[t]he sum of an individual's private life," including his "specific movements down to the minute, not only around town but also within a particular building," could be reconstructed through the data found on a smart phone.[90] When large quantities of data are stored in one place, each individual piece of data—perhaps meaningless on its own—becomes more informative by relation to the other data.[91] *Riley* is the first majority Supreme Court opinion to recognize this mosaic-like effect of cell phone data and its privacy implications.[92]

The *Riley* Court's approach to expectations of privacy was more contextual than binary. The Court refused to view all information found on an arrestee's person as subject to disclosure because of its proximity to the arrestee and because of the arrest itself.[93] Instead, the Court looked at the context of the disclosure and the nature of the information to determine that an arrestee maintained a privacy

86. *Id.* at 2484.

87. *Id.* at 2489. In response to the government's argument that a search of all data stored on a cell phone was materially indistinguishable from searches of physical items, Chief Justice Roberts famously wrote, "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 2488.

88. *Id.* at 2478–89.

89. 132 S. Ct. 945 (2012).

90. *Riley*, 134 S. Ct. at 2489–90 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J. concurring)).

91. *Id*; *see Jones*, 132 S. Ct. at 955.

92. For a definition of "mosaic theory," see Tracey v. State, 152 So.3d 504, 520 (Fla. 2014) ("The theory that discrete acts of surveillance by law enforcement may be lawful in isolation, but may otherwise infringe on reasonable expectations of privacy in the aggregate because they 'paint an "intimate picture" of a defendant's life,' has been referred to as the 'mosaic' theory." (quoting United States v. Wilford, 961 F. Supp. 2d 740, 771 (D. Md. 2013))).

93. *Riley*, 134 S. Ct. at 2488–89.

interest in this immense trove of personal information.[94] Viewed through the lens of Nissenbaum's theory, the inquiry in *Riley* was sensitive to the change in informational attributes between a cigarette pack, which is limited in its ability to contain information, and a cell phone, which has limitless informational value. The Court understood that this difference affected the social norms governing the disclosure of information in each case.[95] While we might expect the physically tangible items we carry in our pockets to be searched and even seized if we are taken into police custody, we do not expect all of the contents of our cell phones—contacts, text messages, emails, documents, pictures—to be disclosed just because we can also carry that data around in our pockets.

Despite the fact that *Riley* explicitly did not overturn the Third-Party Doctrine,[96] at least one lower court has noted its potential impact on future digital privacy cases that do implicate third parties.[97] In *United States v. Guerrero*,[98] the Fifth Circuit upheld the warrantless collection of historical cell site location information ("CSLI") based on the fact that the government obtained the information from a third party.[99] While nothing in *Riley* would allow the Fifth Circuit to ignore the Third-Party Doctrine precedent, the court suggested that perhaps

> the 'technology is different' rationale that led the *Riley* Court to treat an arrestee's cell phone differently from his wallet will one day lead the Court to treat historical cell site data in the possession of a cellphone provider differently from a pen register in the possession of a pay phone operator.[100]

The court added that "commentators have debated the effect *Riley* may have if a 'third party' case involving modern technology were to end up at the Court."[101] The next part of this Recent Development argues that a challenge to law enforcement collection of smart meter data could be just such a case.

94. *Id.* at 2490–91.

95. *See supra* notes 78–79 and accompanying text.

96. *Riley*, 134 S. Ct. at 2489 n.1. *Riley* only concerned the collection of data directly from a person's device and not from a third party, and the fact that the data collection was a search was not at issue. *See id.* at 2484.

97. United States v. Guerrero, 768 F.3d 351, 359 (5th Cir. 2014).

98. 768 F.3d 351 (5th Cir. 2014).

99. *Id.* at 358.

100. *Id.* at 360.

101. *Id.*

III. SMART METERS AND THE FOURTH AMENDMENT

The current application of the Fourth Amendment to utility data ignores the possibility that society might expect the data to be disclosed in certain contexts and not in others. Since utility data is created specifically to be collected by a utility company and can *only* be collected from a third party, all data generated about a household's use of electricity, regardless of its ability to reveal personal information, falls outside of the Fourth Amendment.[102] Utility data concerns information from inside one's home, the core of Fourth Amendment protection.[103] Smart meter data ups the ante by providing infinitely more information about the lifestyles and behaviors of a household's inhabitants.[104] This is a paradigmatic example of how the Third-Party Doctrine subverts society's expectations of privacy by classifying information as either wholly private (if secret) or wholly public (if disclosed).

This Part provides background information on smart meters and the smart grid and discusses the privacy problems associated with smart meters. It then discusses the case law, which reveals that the Third-Party Doctrine has removed Fourth Amendment protection from utility data, including smart meter data. This Part concludes with an argument that a contextual approach to Fourth Amendment expectations of privacy would protect smart meter data from flowing beyond utility companies but for the inharmonious Third-Party Doctrine. Thus, the Supreme Court should follow the trajectory it started with *Riley* and overturn the Third-Party Doctrine.

A. Smart Meters and Privacy

The Energy Independence and Security Act of 2007, Title XIII, established a national policy to modernize electricity transmission and distribution.[105] Part of the policy involves implementing new technologies to increase the amount and flow of information about energy use between consumers and utilities.[106] Taken together, these technologies make up the "smart grid."[107] As part of this effort to

102. *See supra* text accompanying notes 1–11; *infra* text accompanying notes 105–10.

103. Kyllo v. United States, 533 U.S. 27, 42 (2001) (Stevens, J., dissenting) (quoting Payton v. New York, 445 U.S. 573, 586 (1980)).

104. *See* NIST, *supra* note 2, at 26.

105. *See generally* Energy Independence and Security Act of 2007, Pub. L. 110-140, 121 Stat. 1492 (codified at 42 U.S.C. § 17381 (2012)) (including energy independence and security as one of several clean energy goals).

106. 42 U.S.C. § 17381 (2012).

107. *Id.*

modernize the grid, utility companies increasingly are installing smart meters on consumers' homes.[108] In 2011, the U.S. Energy Information Administration reported that more than thirty-three million U.S. utility customers had smart meters.[109] Three million additional smart meters were installed between January and August 2012, and the agency estimated that the number of customers with smart meters would exceed eighty million by 2015.[110]

In many places, smart meter adoption is all but compulsory. Utility companies typically inform the consumer that a smart meter will be installed and then send an employee to install the meter.[111] In 2012, responding to consumer complaints, the California Public Utilities Commission required Pacific Gas and Electric Company to provide consumers in California the option to opt out of smart meter installation.[112] Some other states have opt-out processes, some of which involve charging an opt-out fee.[113] Other states do not provide information or instructions to consumers for opting out.[114]

Smart meters constantly collect fine-grained data on a household's electricity use and transmit the data to the utility companies as frequently as every fifteen minutes.[115] They generate up to 3,000 data points per month per household.[116] The meters are touted as a tool to help consumers save energy and money by keeping track of their energy use patterns over time.[117]

These detailed records of electricity usage can reveal when a person goes to bed every night and wakes up every morning, how

108. *See* ENERGY INFO. ADMIN., *supra* note 3, at 1.

109. *See id.*

110. *Id.* attachment B, 1.

111. 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/.

112. Pac. Gas & Elec. Co., Agenda ID No. 10870, at 40 (Cal. Pub. Util. Comm'n Nov. 22, 2011), *available at* http://docs.cpuc.ca.gov/efile/PD/153864.pdf.

113. Terrence Henry, *Want to Opt Out of a Smart Meter in Texas? It Will Cost You*, NPR (Oct. 30, 2013), http://stateimpact.npr.org/texas/2013/10/30/opt-out-of-a-smart-meter-in-texas-it-will-cost-you/.

114. Duke Energy's smart grid information web pages, for example, do not include information about opting out. *See Grid Modernization FAQs*, DUKE ENERGY, http://www.duke-energy.com/about-us/smart-grid-faq.asp (last visited Jan. 5, 2015).

115. Tracy Idell Hamilton, *Smart-meter Energy Data Now Online*, SAN ANTONION EXPRESS-NEWS (Aug. 20, 2011), http://www.mysanantonio.com/news/energy/article/Smart-meter-energy-data-now-online-2133522.php.

116. Lee Tien, *New "Smart Meters" for Energy Use Put Privacy at Risk*, ELECTRONIC FRONTIER FOUND. (Mar. 10, 2010), https://www.eff.org/deeplinks/2010/03/new-smart-meters-energy-use-put-privacy-risk.

117. *Id.*

many people live in a household, when people are at home and out of town, and even what specific appliance is being used at a given time.[118] Over time, these data can reconstruct a detailed picture of people's behavior and private lives.[119] A Privacy Impact Assessment conducted by the National Institute of Standards and Technology ("NIST") concluded that the data collected by smart meters raise privacy concerns because they can reveal consumers' lifestyle information and information about the use of specific appliances.[120] New smart appliances come with unique "load signatures," which can be identified through the analysis of smart meter data.[121] By recording these load signatures, smart meters can reveal when and for how long a particular appliance was used.[122] This information can provide insight into personal health information such as eating and exercise habits.[123] In a 2012 study in Germany, researchers were able to analyze smart meter data to determine what television programs a household was watching.[124] Thus, smart meter data implicates not only energy usage but also behavioral information and potentially even media consumption and communication records.

As new localities continue to introduce smart meters, the data they collect remains largely unprotected. In its Privacy Impact Assessment, the NIST found a "lack of privacy laws or policies directly applicable to the smart grid."[125] Only a few states have passed laws limiting disclosure of utility data, and no federal law directly addresses this type of information.[126] This treasure trove of information about people's behavior will attract public and private entities alike that want to mine the data for commercial or surveillance purposes.[127] Insurance companies, for example, might want to monitor the activities of households that are covered by their policies.[128] Companies that sell smart appliances may want to monitor

118. NIST, *supra* note 2, at 27.
119. *Id.*
120. *Id.*
121. CDT & EFF Joint Comments, *supra* note 7, at 6.
122. *Id.*
123. *Id.*
124. Robertson, *supra* note 2.
125. NIST, *supra* note 2, at 21.
126. *Id.*; PUB. UTIL. COMM'N OF THE STATE OF CAL., RULEMAKING 08-12-009, ORDER INSTITUTING RULEMAKING TO CONSIDER SMART GRID TECHS. PURSUANT TO FED. LEG. & ON THE COMM'N'S OWN MOT. TO ACTIVELY GUIDE POLICY IN CAL.'S DEV. OF A SMART GRID SYS., 83–87 (July 28, 2011).
127. CDT & EFF Joint Comments, *supra* note 7, at 5.
128. *Id.* at 6.

the use of those appliances for warranty purposes.[129] Some advertisers have already expressed their intent to use this data.[130] WPP, the world's biggest advertising agency, announced that it was teaming up with a London-based software company to study ways to collect smart meter data, saying that it would "open the door of the home."[131] And law enforcement, the focus of this Recent Development, may be interested in collecting smart meter data as part of criminal investigations.[132] Like the cell phone at issue in *Riley*, smart meters can store and transmit, in large quantities, different types of personal information.[133] However, because of the infrastructural design of smart meter technology, law enforcement officers can and do collect this data not from individuals directly but from third-party service providers.[134]

B. Law Enforcement Collection of Utility Data

Law enforcement historically has used energy use records in criminal investigations, usually involving marijuana-growing operations.[135] In the years since *Smith v. Maryland* was decided, courts have relied on the Third-Party Doctrine to hold that no warrant is needed for the collection of these records from utility

129. *Id.*

130. Kantar Group Ltd., whose clients include Coca Cola and Microsoft, is undertaking a pilot study on "ways to harvest smart-meter data on household energy use that may be useful to customers . . . . Companies wanting to market their products . . . could potentially benefit from information [contained in smart meter data], such as how long people spend cooking or using their computers." Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 11, 2014), http://www.bloomberg.com/news/2014-05-11/wpp-unit-onzo-study-harvesting-smart-meter-data.html.

131. Robertson, *supra* note 2.

132. MURRILL ET AL., *supra* note 7, at 2. *See generally* Naperville Smart Meter Awareness v. City of Naperville, No. 11C9299, 2013 WL 1196580 (N.D. Ill. Mar. 22, 2013) (dismissing claim from town's citizens that smart meter installation in every home violates the Fourth, Fifth, and Fourteenth Amendments).

133. *See supra* notes 115–24 and accompanying text.

134. In a 2012 report, California energy company San Diego Gas & Electric reported that it had disclosed the records of 4,062 customers pursuant to the "legal process." SAN DIEGO GAS & ELEC., ANNUAL PRIVACY REPORT 2 (May 16, 2013), *available at* http://www.cpuc.ca.gov/NR/rdonlyres/1AAFED95-3F3F-4296-B4B6-8CB8E6704CC1/0/SDGEAnnual_Privacy_Report_2012.pdf.

135. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001); United States v. Golden Valley Elec. Assoc., 689 F.3d 1108, 1114 (9th Cir. 2012); United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011); State v. Kluss, 867 P.2d 247, 250 (Idaho Ct. App. 1993).

companies.[136] Most of these cases have involved traditional utility records, which show aggregated measures of energy use.[137]

In *United States v. Golden Valley Electric Association*,[138] the Ninth Circuit held that consumers lacked a reasonable expectation of privacy in energy consumption records because they had "no possessory or ownership interest" in the records held by a utility company.[139] In *Golden Valley*, the Drug Enforcement Administration ("DEA") served an administrative subpoena on Golden Valley, an electricity cooperative, to provide energy consumption records pertaining to three customer addresses.[140] Golden Valley, which had a company policy of protecting the confidentiality of members' records, challenged the subpoena on Fourth Amendment grounds.[141] Although the administrative subpoena was subject to relaxed Fourth Amendment standards, the Ninth Circuit addressed the consumers' privacy interest in utility records.[142] Relying on *United States v. Miller*,[143] which involved the collection of bank records, the Court held that "[a] customer ordinarily lacks 'a reasonable expectation of privacy in an item,' like a business record, 'in which he has no possessory or ownership interest.' "[144] The court further concluded that the energy usage records were not "inherently personal or private."[145] Thus, instead of inquiring into society's expectations regarding the disclosures, the Ninth Circuit conceived of utility records as "inherently" not private, based on the fact that they were held by a third party and thus out of the consumers' physical control. It ignored the confidential relationship between the utility company and its customers and the effect of that relationship on the social norms governing the flow of information.

In *Idaho v. Kluss*,[146] the Court of Appeals of Idaho adopted *Smith v. Maryland*'s binary "voluntary disclosure" approach to

136. *See Golden Valley*, 689 F.3d at 1111; *McIntyre*, 646 F.3d at 1113; *Kluss*, 867 P.2d at 249.

137. *See Golden Valley*, 689 F.3d at 1111 (involving power consumption records); *McIntyre*, 646 F.3d at 1113 (involving usage records); *Kluss*, 867 P.2d at 250 (involving power consumption records).

138. 689 F.3d 1108 (9th Cir. 2012).

139. *Id.* at 1116.

140. *Id.* at 1111.

141. *Id.* at 1113.

142. *See id.* at 1115–16.

143. 425 U.S. 435 (1976).

144. *Golden Valley*, 689 F.3d at 1116.

145. *Id.*

146. 867 P.2d 247 (Idaho Ct. App. 1993).

privacy.[147] In *Kluss*, an Idaho Bureau of Narcotics officer obtained defendant Kluss's power consumption information without a warrant from a utility company in order to determine whether Kluss was using special marijuana "grow lights."[148] The officer was able to compare Kluss's consumption to that of the previous residents to determine that Kluss's consumption was high.[149] The officer used this information to obtain a subpoena for the written utility records and a warrant to search Kluss's home.[150] Kluss was ultimately convicted of growing and possessing marijuana.[151] The court held that, under *Smith v. Maryland*, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and thus the Fourth Amendment does not protect utility records.[152] This "voluntary disclosure" approach ignores the context of disclosure and its effect on expectations of privacy. It treats any disclosure to any party for any reason as a voluntary ceding of all privacy protection.

In *United States v. McIntyre*,[153] the Eighth Circuit acknowledged that utility records can reveal normally protected information about the inside of a person's house but still declined to protect that information when law enforcement collected it from a third party.[154] In *McIntyre*, Nebraska State Patrol investigator Jason Sears obtained defendant McIntyre's electricity usage records using an administrative subpoena.[155] Sears discovered a spike in McIntyre's electricity usage for November 2008, which later turned out to be inaccurate, and cited that spike in an affidavit to obtain a warrant for thermal imaging to detect a marijuana growing operation.[156] McIntyre argued that investigators should have obtained a warrant because his utility records "contained intimate details about the interior of his home."[157] The Eighth Circuit reaffirmed that there was no expectation of privacy in information revealed to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[158] The language of *McIntyre* is telling. It reveals the

147. *Id.* at 252.
148. *Id.* at 249–50.
149. *Id.* at 251.
150. *Id.* at 249.
151. *Id.*
152. *Id.* at 252.
153. 646 F.3d 1107 (8th Cir. 2011).
154. *Id.* at 1111.
155. *Id.* at 1109.
156. *Id.* at 1110.
157. *Id.*
158. *Id.* at 1111 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

Third-Party Doctrine's interpretation of the Fourth Amendment as completely divorced from social norms and expectations of confidentiality.

McIntyre argued that "power records are different" because they reveal information about the interior of one's home.[159] He relied on *Kyllo*, arguing that the information obtained was indistinguishable from that in *Kyllo*.[160] The court rejected McIntyre's argument because "the manner in which the information was obtained in *Kyllo*" bore "no resemblance to obtaining power data from a third party."[161] Thus, while *McIntyre* and *Kyllo* both concerned information about the interior of the home, *Kyllo* did not apply because the officers in *McIntyre* could obtain the information from a third party without using "sense-enhancing technology."[162] This interpretation of the Fourth Amendment resembles the outmoded "constitutionally protected areas" doctrine.[163] The court used arbitrary digital boundaries to define expectations of privacy rather than conducting a normative inquiry into society's expectations.[164]

In 2013, the Northern District of Illinois applied the Third-Party Doctrine to smart meter data in *Naperville Smart Meter Awareness v. City of Naperville*.[165] Naperville Smart Meter Awareness ("NSMA"), a coalition of Naperville, Illinois residents who were required to have smart meters installed at their homes or businesses, sought to enjoin Naperville from installing the smart meters until reasonable privacy safeguards were in place and a satisfactory alternative option for all customers was available.[166] The court extended *Smith v. Maryland*, finding that the residents consented to having their information monitored by transmitting it to the utility company.[167] *Naperville* did not involve the collection of information *from* a third party—the objected-to collection was *by* the third party itself. By extending the Third-Party Doctrine in this case, the court equated plaintiffs' knowledge of the data collection with consent, even though the plaintiffs were suing in objection to the collection itself. This rationale is an example of a "well-known logical trap" in which the knowledge of data collection is equated with the inability to expect privacy in the

159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*
163. *See supra* notes 32–34 and accompanying text.
164. *See McIntyre*, 646 F.3d at 1111.
165. No. 11 C 9299, 2013 WL 1196580, at *1 (N.D. Ill. Mar. 22, 2013).
166. *Id.*
167. *Id.* at *11.

data.[168] The knowledge-as-consent rationale is particularly counterintuitive in the case of utility meters, which are necessary fixtures for most people who use electricity.[169]

The cases applying the Third-Party Doctrine to utility data take a binary approach to information privacy. Even though customers disclose their data only to the utility company for the limited purpose of billing, this limited disclosure exempts the information from Fourth Amendment protection. Reasonable assumptions about confidentiality between the consumer and the utility company do not bear on the courts' inquiry into whether a reasonable expectation of privacy exists. This approach is contrary to that in *Riley*, which recognized that the specific context of a disclosure—not the storage method or vulnerability of the data to collection—determines whether society expects privacy.[170]

C. A Contextual Approach to Smart Meter Privacy

This Recent Development has argued that *Riley* adopted a much-needed contextual approach to digital privacy by (a) acknowledging that digital data, stored and aggregated in large quantities, can reveal a detailed picture of an individual's private life, imbuing each individual piece of data with an informational value that it might not have had standing alone, and (b) refusing to equate the vulnerability of information with a loss of privacy interests. Applying the same principles to smart meter data would support its protection under the Fourth Amendment.

168. Selbst, *supra* note 13, at 659.

169. For a discussion of the consent rationale in the cell phone context, see *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126–27 (E.D.N.Y. 2011) (noting that, because of the ubiquity and necessity of the cell phone in modern society, "[t]he fiction that the vast majority of the American population consents to warrantless government access to [cell site location records] by 'choosing' to carry a cell phone must be rejected").

170. *See* Riley v. California, 134 S. Ct. 2473, 2488–91 (2014) ("The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. Not every search is acceptable solely because a person is in custody. To the contrary, when privacy-related concerns are weighty enough, a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee. . . . The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from search of [physical items such as cigarette packs]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. . . . A conclusion that inspecting the contents of an arrestee's pocket works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.").

The type of information that can be learned from collecting and analyzing smart meter data lies at the core of Fourth Amendment protection.[171] Smart meters implicate privacy by aggregating hundreds of thousands of data points that together reconstruct the behavioral patterns of a household.[172] Law enforcement already uses traditional utility data to learn information from inside the home, and smart meters would only increase the amount, types, quality, and accuracy of information available to law enforcement.[173] Information inside the home is the paradigmatic example of the Fourth Amendment-protected sphere.[174] In *Katz*, the Court abandoned the "constitutionally protected areas" that limited warrant requirements to physical intrusions into the home.[175] In *Kyllo*, it confirmed that the use of an electronic device to obtain such information was a Fourth Amendment search.[176] In *Riley*, the Court found that the search of a cell phone, with its large capacity to store many different types of data, was similar to searching one's home.[177] Like a cell phone, smart meters are designed to collect vast amounts of digital data from inside the home—data that is even more revealing than that obtained by the heat sensors used in *Kyllo*. Smart meters combine the newer digital mosaic concerns raised in *Riley* with the time-tested privacy of the home as enshrined in the Fourth Amendment's history. Through smart meters, information once protected by physical boundaries now flows electronically and is aggregated in a way that it could not have been before this technology existed. The question of smart meter privacy thus demonstrates the need for Fourth Amendment standards to adapt to protect traditional privacy concerns in the digital age.

Under the Third-Party Doctrine, the type of information collected by smart meters would be protected if obtained without a warrant directly from a person's home, but not from a third-party utility company. This binary public/private conception of the Fourth Amendment is a regression to the "constitutionally protected areas" doctrine abandoned in *Katz*—that is, the idea that information is private only if stored in a protected, "private" place.[178] A contextual approach to privacy, like the one adopted in *Riley*, requires asking not

171. Kyllo v. United States, 533 U.S. 27, 30–31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

172. NIST, *supra* note 2, at 5; Robertson, *supra* note 2.

173. MURRILL ET AL., *supra* note 7, at 5.

174. *Kyllo*, 533 U.S. at 38.

175. United States v. Katz, 389 U.S. 347, 351 n.9 (1967).

176. *Kyllo*, 533 U.S. at 40.

177. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

178. *See supra* text accompanying note 175.

whether the information was obtained from a protected area or whether it was "inherently" private, but whether society would expect the information to have the potential to be exposed in a particular context. It requires asking whether, upon having a meter installed that automatically relays energy usage data to a utility company for billing purposes, a person expects that the data can be shared with law enforcement and other agencies without additional consent or a warrant.

Under a contextual lens, the role of the home as a social institution is one of solitude and seclusion.[179] Thus, warrantless collection of information from inside the home typically violates social norms. Other evidence provides additional insight into the social norms that govern the transmission of smart meter data. Smart meter data is transmitted to the utility company for billing purposes and to help both the utility and the household manage electricity use.[180] Evidence from the case law surrounding smart meters suggests that customers may, at least implicitly, expect a utility company to maintain confidentiality in energy usage data.[181] California's reporting requirements and the response to recent reports of disclosures suggest that the disclosure of an individual's smart meter data to a third party without express consent violates social norms.[182] Thus, social norms in the context of smart meter data would prohibit the data from flowing beyond the utility company.

While the Third-Party Doctrine is couched in the language of "reasonable expectations," it never actually examines them. Instead, it equates the "voluntary" disclosure of data to a third party for a specific business purpose with consent to disclose the same data to law enforcement.[183] If the information flows to any third party for any reason, all privacy is forfeited. This approach resembles the outmoded "constitutionally protected areas" doctrine in its reliance on binary distinctions. However, even the "constitutionally protected areas" approach placed paramount importance on the privacy of the

179. *See infra* note 182 and accompanying text.

180. *See supra* notes 115–17 and accompanying text.

181. United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012) (noting that Golden Valley had "a company policy of protecting the privacy of its members," but finding no "agreement with its customers" to that effect). Even in the absence of an explicit confidentiality agreement, Golden Valley's contention suggests that utility companies and customers may implicitly assume a confidential relationship. Regardless of whether the law would support such a relationship, this indicates at least a subjective expectation of confidentiality. *Id.*

182. SAN DIEGO GAS & ELEC., *supra* note 134.

183. *See supra* text accompanying notes 167–68.

home, a concept that has endured throughout the history of Fourth Amendment jurisprudence.[184] Privacy scholar Andrew Selbst argued that the privacy of the home is an area that "would generate a consensus between" traditional Fourth Amendment analysis and a contextual approach to privacy.[185] Under current law, "courts have said that the 'home' is such a quintessentially private place that physical intrusion even by a 'fraction of an inch' is too much."[186] Under Selbst's contextual analysis, "the home is a specific social context . . . subject to the transmission principle of *control by the resident*."[187] Allowing unwarranted intrusion in this context "would destroy the home as a social institution, generally seen as the one place it is always safe to retreat."[188] Applying the Third-Party Doctrine to smart meter data, as Selbst warns, would erode the integrity of the home by exposing the activities and behavioral patterns of its residents.[189] In the case of smart meters, the Third-Party Doctrine is thus incongruous not only with a contextual approach to privacy but also with longstanding Fourth Amendment values.

CONCLUSION

This Recent Development has argued that *Riley*'s approach to digital data, although it did not address the Third-Party Doctrine, will inevitably lead to the doctrine's undoing. In *Riley*, the Supreme Court acknowledged that old ideas about expectations of privacy do not hold up when law enforcement collects digital data.[190] Because an arrestee's pocket, which was once fair game for container searches, can now hold information in digital form about every aspect of the arrestee's life, the context of that pocket and the social norms surrounding it have changed. Because Third-Party Doctrine's binary approach to digital privacy does not accommodate such changing circumstances and norms, it will produce results that are contrary to basic reason and Fourth Amendment values, such as protecting data that is saved to a hard drive but not protecting the same data saved to

184. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("[P]hysical invasion of the structure of the home, 'by even a fraction of an inch,' [is] too much . . . ." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

185. Selbst, *supra* note 13, at 668.

186. *Id.* at 667 (quoting *Kyllo*, 533 U.S. at 37).

187. *Id.* at 667–68.

188. *Id.* at 668.

189. *Id.* at 668–69.

190. *See* Riley v. California, 134 S. Ct. 2473, 2888–91 (2014).

a cloud storage account. This incongruity is perhaps most apparent in the context of smart meters, where, under the Third-Party Doctrine, the Fourth Amendment fails to protect the home—the original impetus for the right to privacy.

NATASHA H. DUARTE**

**The author would like to thank Cathy Packer, Brooks Fuller, Anne Klinefelter, Woodrow Hartzog, Astrid Duarte, Tony Duarte, Alison Templeton, and the *North Carolina Law Review* board and staff.