SMART METERS AS A CATALYST FOR PRIVACY LAW

Matthew Tokson[*]

Smart utility meters raise several puzzling legal questions and answering them can help point the way toward the future of Fourth Amendment and civil privacy law. This Response expands on two such issues: use restrictions on collected data, and voluntary data disclosure.

More than any other current technology, smart meters compel the development of use restrictions on collected data. The benefits of smart meters are potentially enormous, such that categorically prohibiting public utilities from collecting smart meter data is likely beyond the pale.[1] Yet allowing law enforcement agents to obtain such intimate data about the home without a warrant seems equally unacceptable. Smart meters are currently the clearest example of the need for robust restrictions on how the government can use data it has collected. Government entities are already collecting detailed personal information about citizens for a variety of legitimate, non-law enforcement purposes.[2] Limiting access to such data will often be the best practical means to ensure citizen privacy in the era of big data.

Smart meter privacy is threatened by legal regimes that emphasize users' voluntary disclosure of their energy use data. While many customers have little choice but to use smart meters, numerous others do have a choice, and detailed energy surveillance likely entails customers voluntarily choosing to link their smart meters with smart home devices and appliances. Under some doctrinal approaches, such voluntarily disclosed data would be wholly unprotected by the Fourth Amendment.[3] Courts and scholars would do well to move beyond existing paradigms of voluntary choice and inescapable surveillance, lest the most sensitive forms of smart meter data remain unprotected.

Professor Matthew Kugler and Meredith Hurley's sophisticated analysis of smart meter privacy provides a valuable roadmap for scholars and lawmakers as they confront the novel questions posed by smart meters.[4] This Response seeks to expand on Kugler and Hurley's analysis

---

* Professor of Law, University of Utah S.J. Quinney College of Law. Thanks to Matthew Kugler for helpful comments, and thanks to Matthew Nepute for excellent research assistance.

1. Matthew B. Kugler & Meredith Hurley, *Protecting Energy Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 451, 453–55 (2020).

2. *See, e.g.*, Kugler & Hurley, *supra* note 1, at 453; Jennifer D. Oliva, *Prescription-Drug Policing: The Right to Health-Information Privacy Pre- and Post-*Carpenter, 69 DUKE L.J. 775, 780 (2020) (noting that many states have implemented prescription-drug monitoring programs, which collect sensitive data on patients who fill controlled substance prescriptions).

3. Kugler & Hurley, *supra* note 1, at 476–77; Orin S. Kerr, *Implementing* Carpenter, 20-22, (USC Law Legal Studies, Working Paper No. 18-29, 2018), https://ssrn.com/abstract=3301257 [https://perma.cc/5YSD-7H5S].

4. Kugler & Hurley, *supra* note 1, at 452. Kugler and Hurley's detailed and insightful account of smart meter privacy also touches on important issues like the public/private distinction

of use restrictions and to reimagine their approach to voluntary data disclosure.

I. THE ERA OF USE RESTRICTIONS BEGINS

Since the beginning of the twenty-first century, scholars have debated whether the law should regulate how law enforcement agents *use* government data, in addition to regulating data *collection*.[5] There are two central controversies in this literature: first, whether use restrictions are effective at protecting privacy;[6] and second, if they are effective, whether they should be imposed primarily by courts or legislatures.[7] Some have argued that use restrictions can effectively protect privacy in a variety of contexts,[8] while others contend that such restrictions will be difficult to implement and may weaken restrictions on data collection.[9] Likewise, some scholars favor leaving use restrictions to legislatures, arguing that Fourth Amendment doctrine as applied by courts is a poor fit for such granular restrictions;[10] others have proposed that Fourth Amendment law can provide a coherent foundation for use restrictions.[11]

There are strong arguments on both sides of these issues.[12] But for better or worse, events have largely overtaken these debates and may soon render them irrelevant. The era of use restrictions has already begun. Smart utility meters are the perfect illustration of this phenomenon. As Kugler and Hurley demonstrate, the benefits of smart meters are potentially massive.[13] Smart meters are necessary for efficient energy

---

in Fourth Amendment law, the Federal Trade Commission's (FTC) strengths and weaknesses as a privacy regulator, data mining regulations for private companies, and the meaning of the landmark decision, *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *See* Kugler & Hurley, *supra* note 1, at 497–98, 507.

5. *E.g.*, Wayne A. Logan, *Policing Police Access to Criminal Justice Data*, 104 IOWA L. REV. 619, 625 (2019); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 580 (2017); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 179 (2017); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 64 (2014); Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law*, *in* FUTURE OF THE CONSTITUTION 3 (Brookings Inst., 2011), https://www.brookings.edu/research/use-restrictions-and-the-future-of-surveillance-law/ [https://perma.cc/4SNH-XVSE]; William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2160 (2002); Matthew Tokson, *Inescapable Surveillance*, 105 CORNELL L. REV. 409, 418–19 (2021).

6. Several scholars have argued compellingly in favor of use restrictions, *see, e.g.*, Joh, *supra* note 5, at 64; Kerr, *supra* note 5, at 8, while others have offered strong arguments that use restrictions are likely to be ineffective, Simmons, *supra* note 5, at 179–194.

7. *Compare* Kerr, *supra* note 5, at 8, *with* Logan, *supra* note 5, at 664.

8. *E.g.*, Kerr, *supra* note 5, at 8; Joh, *supra* note 5, at 64.

9. Simmons, *supra* note 5, at 179–94.

10. Simmons, *supra* note 5, at 180–82; Kerr, *supra* note 5, at 9–10.

11. *E.g.*, Logan, *supra* note 5, at 664; Berman, *supra* note 5, at 580.

12. *See supra* notes 6–11.

13. Kugler & Hurley, *supra* note 1, at 460–69.

grid management, which may be indispensable for addressing climate change and furthering general prosperity.[14] Prohibiting public or quasi-public utilities from using smart meters is likely not viable as a policy choice under current circumstances.[15] At the same time, there are substantial and growing privacy risks from smart meter data, which is capable of disclosing detailed information about the activities of people inside a home.[16] For example, smart meters can reveal to the government what devices a resident is using, the time and duration of use, and potentially more.[17] Permitting law enforcement agents unfettered access to details about a person's activities inside their home disregards core constitutional values.[18]

In addressing this dilemma, courts and lawmakers have begun to rely on use restrictions that permit government utilities to obtain sensitive data about homeowners but prohibit the dissemination of such data to other agencies without a court order.[19] These use restrictions go far beyond familiar limitations on the scope of warrants.[20] In *Naperville Smart Meter v. City of Naperville*, the Seventh Circuit upheld a town's use of mandatory smart meters on the ground that their data collection was "unrelated to law enforcement" and was otherwise reasonable.[21] Importantly, the court noted that its holding depended on the particular circumstances of the case, and that "our conclusion might change if the data was more easily accessible to law enforcement or other city officials outside the utility."[22] This statement, and the court's repeated emphasis

14. Kugler & Hurley, *supra* note 1, at 457. Smart meters also help utilities address outages and generate sufficient power, and help consumers save money and adopt energy-efficient behaviors. *Id.* at 464–66.

15. *See* Kugler & Hurley, *supra* note 1, at 457; *see generally* IPCC, SPECIAL REPORT ON THE OCEAN AND CRYOSPHERE IN A CHANGING CLIMATE, (2019) (explaining the immediate effects of climate change and the urgency of its mitigation).

16. Kugler & Hurley, *supra* note 1, at 469–70.

17. Kugler & Hurley, *supra* note 1, at 469–72 (discussing the possibility that smart meters may become integrated with smart home devices such as Amazon Echo, smart lights and thermostats, or smart TVs).

18. Kugler & Hurley, *supra* note 1, at 469–74.

19. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018) (finding that Naperville's data collection did not violate the Fourth Amendment specifically because of this use restriction).

20. *See, e.g.*, California v. Riley, 573 U.S. 373, 386 (2014) (prohibiting police from searching a cell phone's contents under the traditional search incident to arrest exception); United States v. Sedaghaty, 728 F.3d 885, 913 (9th Cir. 2013) (requiring an additional warrant to permit a further search of computers seized for a different search); United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (finding that police exceeded the scope of a private search when they examined disks that the private searchers did not examine).

21. Naperville, 900 F.3d at 529. *See also id.* at 528 ("Critically, Naperville conducts the search with no prosecutorial intent. Employees of the city's public utility—not law enforcement—collect and review the data.").

22. Naperville, 900 F.3d at 529.

on the non-law enforcement use of the data, strongly indicates that it would reverse course if the city started sharing data with law enforcement. The Seventh Circuit functionally imposed a Fourth Amendment use restriction on the data. Going forward, in the Seventh Circuit, smart meter data collection is only reasonable under the Fourth Amendment so long as it is walled off from law enforcement uses.[23]

Another recent case suggests that courts may also directly impose restrictions on law enforcement requests for data held by other government agencies. This would extend the principle of *Naperville* beyond smart utility programs, providing Fourth Amendment protections for a variety of non-law-enforcement government databases. In *United States v. Hasbajrami*, the Second Circuit ruled that the Fourth Amendment applies to law enforcement use of data collected and stored by other government agencies.[24] FBI agents had queried a national security database of emails and other communications with foreign nationals collected by the NSA under the Foreign Intelligence Surveillance Act of 1978.[25] The Second Circuit remanded to the district court to determine whether this additional use was reasonable under the Fourth Amendment.[26] It noted that the enormity of the communications database and the sensitive nature of the data compelled constitutional restrictions on use, lest the program turn into a limitless source of domestic surveillance.[27] If law enforcement could query such a vast database without any constitutional check, it would be akin to a general warrant allowing the government to search wherever and whomever it pleases—the precise evil that the Fourth Amendment was designed to prevent.[28] The court indicated that domestic law enforcement queries of the NSA's vast foreign intelligence database would likely raise serious constitutional concerns.[29]

The *Hasbajrami* opinion leaned heavily on recent Supreme Court cases expanding the scope of the Fourth Amendment to cover digital databases held by third parties and imposing limits on searching cell

23. *See id.* at 528–29.

24. United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019) ("[Q]uerying that stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable. Our reasoning is based on three considerations.").

25. *Id.* at 645.

26. *Id.* at 661.

27. *Id*. at 671.

28. *Id.* ("If such a vast body of information is simply stored in a database, available for review by request . . . the program begins to look more like a dragnet, and a query more like a general warrant . . . ."); Kugler & Hurley, *supra* note 1, at 482.

29. Hasbajrami, 945 F.3d at 672.

phones lawfully seized during an arrest.[30] Indeed, the recent expansion of the scope of the Fourth Amendment in *Carpenter v. United States* is essential to the rise of use restrictions.[31] Prior to *Carpenter*, most information disclosed to a third party was wholly unprotected by the Fourth Amendment, making the imposition of use restrictions impossible in most cases.[32] But today, such information may be protected by the Fourth Amendment, and both *Naperville* and *Hasbajrami* relied on this expanded protection in their analyses.[33]

Finally, the fact that courts are applying Fourth Amendment use restrictions to collected data does not mean that there is no place for statutory use restrictions. Indeed, Naperville city regulations providing that its public energy utility would not provide customer data to law enforcement officers without a search warrant reassured the Seventh Circuit that Naperville's regime was constitutional.[34] And Kugler and Hurley's proposed Energy Use Privacy Act would, among its many appealing provisions, limit access to smart meter utility data to the utility itself.[35] Further, Fourth Amendment use restrictions are likely to work best when they impose simple, bright-line restrictions on use, such as prohibiting all law enforcement uses while permitting all non-law-enforcement uses.[36] More sophisticated or nuanced use restrictions are better suited for implementation by statute.[37] Likewise, restrictions on the dissemination of smart meter data to private entities will require statutes that protect consumer privacy against commercial exploitation.[38]

Regardless of whether statutory restrictions might be optimal, the extremely slow pace of federal privacy legislation and the weak or absent nature of state statutes thus far likely means courts will need to develop use restrictions in Fourth Amendment law—or fail to restrain government database use at all.[39] The most pressing question involving use

30. *Id.* at 671–72; Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Riley v. California, 573 U.S. 373, 386 (2014).

31. Carpenter, 138 S. Ct. at 2223.

32. Kerr, *supra* note 5, at 9–10.

33. Naperville, 900 F.3d at 527; Hasbajrami, 945 F.3d at 671–72.

34. Kugler & Hurley, *supra* note 1, at 494 (describing Naperville's "Smart Grid Customer Bill of Rights" law, which prohibits the provision of customer data to law enforcement without a court order).

35. Kugler & Hurley, *supra* note 1, at 504.

36. Another possibility would be limiting all uses to the collecting agency and prohibiting access from any other agency.

37. *See* Kerr, *supra* note 5, at 10 (noting that legislatures have advantages over courts in developing detailed use restrictions).

38. Kugler & Hurley, *supra* note 1, at 496.

39. *See* Kugler & Hurley *supra* note 1, at 505 (discussing the weak protections offered by those few state statutes that exist); Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 797 (2019); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 192–93 (2016).

restrictions is no longer whether they will occur, or who will implement them, but rather how courts and (eventually) lawmakers can best apply them to novel information-gathering technologies. Smart meters provide a path-making example of a technology that compels use restrictions on gathered data, and the brief history of smart meter implementation suggests that courts and lawmakers can successfully impose such restrictions.

II. INESCAPABLE SURVEILLANCE AND VOLUNTARY DISCLOSURE

Traditionally, the Fourth Amendment has granted no protection to information that a person shares with third parties.[40] The Supreme Court recently reshaped this "third-party doctrine" in *Carpenter v. United States*, which established that people retain a Fourth Amendment right in their cell phone location data even though it is revealed to others.[41] *Carpenter* is a notably ambiguous case and its precise meaning going forward is contested.[42] Some scholars believe *Carpenter* is the first step in a revolutionary expansion of Fourth Amendment protection to new forms of digital data,[43] while others consider it a more limited exception to the third-party doctrine for certain types of surveillance.[44]

One issue central to this debate is the importance of voluntary disclosure, such as whether an individual chooses to disclose their data to a third party or whether such disclosure is largely inescapable. In the wake of *Carpenter*, many scholars and lower courts have endorsed voluntary disclosure as an important factor in determining Fourth Amendment rights.[45] Some have gone further and argued that information

---

40. Kugler & Hurley *supra* note 1, at 476; Tokson, *supra* note **Error! Bookmark not defined.**, at 415–18.

41. Tokson, *supra* note **Error! Bookmark not defined.**, at 409.

42. *See, e.g.*, Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 136 Harv. L. Rev. (forthcoming 2022); Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision —* Carpenter v. United States, CONCURRING OPINIONS (June 22, 2018), https://web.archive.org/web/20180721111755/https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-states.html. [https://perma.cc/Y94X-PTXR]; Orin S. Kerr, *First Thoughts on Carpenter v. United States*, THE VOLOKH CONSPIRACY (June 22, 2018), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta/ (discussing the many important questions left open by the *Carpenter* opinion); Kugler & Hurley, *supra* note 1, at 496 ("*Carpenter* . . . raised questions about dozens of issues and it may be years before courts give clear answers to any of them.").

43. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 357, 386 (2019).

44. Kerr, *supra* note 3, at 17.

45. Ohm, *supra* note 43, at 385; Kerr, *supra* note 3, at 20–22. United States v. Sigouin, 494 F. Supp. 3d 1252, 1265 (S.D. Fla. 2019); United States v. Diggs, 385 F. Supp. 3d 648, 660–61 (N.D. Ill. 2019). *But see* Tokson, *supra* note **Error! Bookmark not defined.**, at 425–39.

voluntarily disclosed to third parties is *never* protected.[46] Such an approach would narrowly limit the scope of *Carpenter* and leave a wide variety of personal information unprotected by the Fourth Amendment.[47]

Kugler and Hurley largely adopt this restrictive view, arguing the view "appear[s] to be inherent in the language of *Carpenter*."[48] Thus, an individual seeking Fourth Amendment protection would need to show that the collection of their data was unavoidable and not the result of a voluntary choice.[49] Fortunately, smart meter data often passes this test.[50] Residents whose utilities adopt smart meters may have no choice but to use such meters in their homes.[51] Those residents cannot be said to have voluntarily disclosed their data to a third party; the collection of their data was largely inescapable.[52]

But in a world where only involuntarily disclosed data is protected, even smart meter data is vulnerable and existing Fourth Amendment protections for such data can be easily circumvented. The more closely one examines the smart meter context, the less confident one becomes that such data would be protected under an "involuntary disclosure only" paradigm.

Not all smart meter installations are mandatory. Many states and municipalities permit their users to opt out of smart meters, some for no fee.[53] In the numerous jurisdictions with opt outs and non-exorbitant fees, the disclosure of one's smart meter data to the government is a voluntary

---

46. *See* Kerr, *supra* note 3, at 20–22; United States v. Shipton, No. 0:18-CR-202-PJS-KMM, 2019 WL 5330928, at *14 (D. Minn. Sept. 11, 2019), report and recommendation adopted, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019) (leaning heavily on voluntariness in holding that peer-to-peer file sharing is unprotected by the Fourth Amendment).

47. Tokson, *supra* note **Error! Bookmark not defined.**, at 413–15. *See also, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (holding that the use of a messaging app was voluntary and therefore data associated with its use was unprotected); United States v. Kidd, 394 F. Supp. 3d 357, 358–59, 365–66, (S.D.N.Y. 2019) (holding that a voice-over-internet-protocol service was not ubiquitous or inescapable and therefore was likely not protected by the Fourth Amendment).

48. Kugler & Hurley, *supra* note 1, at 486–87. This conclusion is controversial, and the importance of involuntary disclosure to *Carpenter*'s outcome is unclear. *See* Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L. J. 1, 5–6 (2020). The Court's discussion of the voluntariness issue takes up a single paragraph in a lengthy opinion that mostly focuses on the "detailed, encyclopedic, and effortlessly compiled" nature of cell phone surveillance and its potential negative effects on citizen privacy. Carpenter v. United States, 138 S. Ct. 2206, 2211–12, 2215–19, 2216 (2018).

49. Kugler & Hurley, *supra* note 1, 486–87 (citing Kerr, *supra* note 3, at 3).

50. Kugler & Hurley, *supra* note 1, at 486–87.

51. Kugler & Hurley, *supra* note 1, at 453.

52. Kugler & Hurley, *supra* note 1, at 486–87.

53. *See Smart Meter Opt-Out Options and Fees*, ELECTRONIC SILENT SPRING, (last updated Nov. 6, 2016) https://www.electronicsilentspring.com/wp-content/uploads/2014/01/SMART-METER-OPT-OUT-OPTIONS-AND-FEES-by-STATE.pdf [https://perma.cc/AU2A-5AZY].

choice—and this intimate data might be unprotected.[54] While homeowners in Portland (where opting out is prohibitively expensive)[55] would enjoy privacy in their smart meter data, homeowners in Los Angeles (where opting out is free) may not.[56] Nor are those Los Angeles homeowners likely to opt out because default rules exert a powerful influence and opting out is rare in virtually every consumer context.[57] Of course, if the vast majority of people do adopt smart meters, that may demonstrate their societal ubiquity and make it more likely that they will be protected under *Carpenter*.[58] But the precise meaning of *Carpenter* remains unclear, and a consumer's voluntary adoption of smart meters in the face of easy opt outs might be enough to preclude Fourth Amendment protection.[59] Governments seeking to obtain smart meter data could provide low-fee opt outs, potentially eliminating the involuntary nature of smart meter data disclosure.

Further, the most concerning forms of smart meter data collection likely involve voluntary consumer choices, which would eliminate Fourth Amendment protection under Kugler and Hurley's adopted framework.[60] Kugler & Hurley express particular concern about smart meters that are connected to various smart appliances and devices like Amazon's Alexa.[61] The integration of these devices with a smart meter system can reveal even more about the intimate activities of the home.[62] Yet integrating smart home devices with smart meters is an inherently voluntary act. Purchasing smart home devices in itself is voluntary, and indeed only about one-fourth of American households currently contain such devices.[63] Moreover, integrating these devices' data-gathering capabilities with smart meters is likely to be a voluntary step that requires

---

54. *See* Kerr, *supra* note 3, at 20–22.

55. I refer here to Portland, Oregon, where, as of late 2016, opt-out fees were $254 plus an ongoing monthly surcharge of $51. *See supra* note 53.

56. *See supra* note 53.

57. *See, e.g.*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 83 (2008).

58. Carpenter v. United States, 138 S. Ct. 2206, 2211, 2220 (2018) (noting the ubiquity of cellphones and characterizing them as indispensable to participation in modern society).

59. *See* Tokson, *supra* note 42 (reporting that lower courts generally focus on the automatic and involuntary nature of data disclosure, rather than the ubiquity of a technology, when applying *Carpenter*).

60. *See* Kugler & Hurley, *supra* note 1, at 486–87.

61. Kugler & Hurley, *supra* note 1, at 472 (noting that these devices "can be connected to or integrated with the home energy management system.").

62. Kugler & Hurley, *supra* note 1, at 473–74.

63. Micah Singleton, *Nearly a quarter of US households own a smart speaker, according to Nielsen*, THE VERGE (Sep. 30, 2018), https://www.theverge.com/circuitbreaker/2018/9/30/17914022/smart-speaker-40-percent-us-households-nielsen-amazon-echo-google-home-apple-homepod [https://perma.cc/VG6F-PPHU].

conscious action on the part of a homeowner.[64] Data obtained from smart speakers and other devices integrated with smart meters would accordingly be unprotected by the Fourth Amendment, despite its especially intimate, detailed, and voluminous nature.

Voluntariness paradigms provide a shaky foundation for smart meter privacy. Between opt-out opportunities and the voluntary nature of smart device integration, the robust Fourth Amendment protections that Kugler and Hurley contemplate may be substantially diminished.[65] In this respect, smart meter data is in good company, joining numerous other forms of digital data that would go unprotected or underprotected under a voluntariness approach: ride-sharing data, individual website data, peer-to-peer file sharing, DNA analysis, smart phone apps including dating and other personal apps, smart home devices, and more.[66]

An involuntariness requirement is hardly inevitable. Most scholars view involuntariness not as a requirement but as merely one factor among many examined in *Carpenter*.[67] The Court's discussion of the voluntariness issue in *Carpenter* was mostly confined to a single paragraph in a lengthy opinion that largely focused on factors such as the deeply revealing nature of the surveillance, the amount of data gathered, the number of persons affected, and the cost of the surveillance.[68]

Voluntariness need not be definitive in future cases. Lower courts applying *Carpenter* have sometimes examined the voluntary or inescapable nature of data disclosure and other times ignored this consideration.[69] Factors such as revealing nature and amount are

64. *See* Kugler & Hurley, *supra* note 1, at 507 (discussing the development of consumer products that will interact with smart meters, thereby enhancing the value of the smart grid).

65. *See* Kugler & Hurley, *supra* note 1, at 489.

66. Tokson, *supra* note **Error! Bookmark not defined.**, at 433–37. *See also, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (holding that the use of a messaging app was voluntary and therefore data associated with its use was unprotected); United States v. Kidd, 394 F. Supp. 3d 357, 358–59, 365–66, (S.D.N.Y. 2019) (holding that a voice-over-internet-protocol service was not ubiquitous or inescapable and therefore was likely not protected by the Fourth Amendment); United States v. Shipton, No. 0:18-CR-202-PJS-KMM, 2019 WL 5330928, at *14 (D. Minn. Sept. 11, 2019), report and recommendation adopted, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019) (holding that the government could monitor peer-to-peer file sharing because file sharing was not indispensable to daily life and required a voluntary action by the user).

67. *See* Ohm, *supra* note 43, at 378, 384; Tokson, *supra* note 48, at 5; Susan Freiwald and Stephen W. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 207 (2018).

68. Carpenter v. United States, 138 S. Ct. 2206, 2216, 2211–12, 2215–19 (2018).

69. *See supra* note 66; United States v. Howard, 426 F. Supp. 3d 1247, 1256–58 (M.D. Ala. 2019) (holding that one-day warrantless GPS tracking did not violate the Fourth Amendment because it was shorter in duration and less revealing than cell phone tracking); United States v. Kelly, 385 F. Supp. 3d 721, 726–27 (E.D. Wis. 2019) (holding that the government could warrantlessly capture video from the hallway of an apartment building which was not the defendant's residence because the camera collected little information and the information

generally more prevalent in post-*Carpenter* decisions.[70] Moreover, some scholars have argued that voluntariness is a conceptually incoherent standard that should be minimized by lower courts and ultimately abandoned by the Supreme Court.[71] In any event, by relying less on the involuntary nature of smart meter disclosure and more on the revealing nature and amount of data that smart meters collect, Kugler and Hurley could further strengthen their arguments that such data should receive Fourth Amendment protection.

CONCLUSION

This Response has argued that smart meters and the questions they raise can help point the way toward the future of privacy law. First, the unique characteristics of smart meters compel judicial and legislative use restrictions as no technology has before. Second, voluntariness paradigms offer only partial and unstable Fourth Amendment protection for smart meter users, and these paradigms should be abandoned for broader and more inclusive approaches. Kugler and Hurley offer an excellent and thorough analysis of the privacy considerations at stake in the smart meter context. The Energy Use Privacy Act they propose would substantially promote smart meter privacy against government and private actors. Ultimately, their illuminating discussion and innovative solutions will help courts and lawmakers accommodate this important new technology while preserving residential privacy.

---

captured was not sensitive); United States v. Jenkins, No. 1:18-CR- 181-MLB-CMS, 2019 WL 2482171, at *2 (N.D. Ga. Feb. 5, 2019) (finding that the basic subscriber information associated with a user's internet accounts was less revealing and involved far less data than cell phone tracking, and was therefore not a Fourth Amendment search), *report and recommendation adopted*, No. 1:18- CR-00181, 2019 WL 1568154 (N.D. Ga. Apr. 11, 2019); People v. Tafoya, 2019 COA 176, ¶¶ 42–48 (ruling that video surveillance of the curtilage of a suspect's home for a three-month period violated the Fourth Amendment because such monitoring captured a great deal of information over time and could reveal sensitive details about a person's life). These opinions do not overtly reject the concept of inescapability, but they do resolve novel Fourth Amendment questions without addressing it.

70. Tokson, *supra* note 42.

71. Tokson, *supra* note **Error! Bookmark not defined.**, at 426–33.