ALEXA: CAN YOU KEEP A SECRET?
THE THIRD-PARTY DOCTRINE IN THE AGE OF THE SMART HOME

Grace Manning*

INTRODUCTION

Under the Fourth Amendment, the home is a castle.[1] It is the place where one may retreat and "be free from unreasonable governmental intrusion."[2] It is afforded the highest level of protection.[3] Not so with the smart home. In the home enhanced by artificial intelligence, there is no reasonable expectation of privacy in data shared with third parties like Amazon.[4] The third-party doctrine says there is no expectation of privacy in information voluntarily provided to others.[5]

The Fourth Amendment protects the right to be secure in one's person, house, papers, and effects, against unreasonable searches and seizures.[6] In recent years, the Amendment has taken on new meaning. Today, we mail our DNA – the very essence of our persons – to 23andMe. We rely on Alexa in our houses, and her always-on microphone[7] to make life easier. We store our papers and effects on the Cloud, in Gmail, and on Dropbox. Focusing on Alexa, this article will contend that the third-party doctrine no longer comports with the Fourth Amendment. Nixing the doctrine – and replacing it with robust privacy protections – is the only way forward.[8]

---

* Grace Manning is a *juris doctor* candidate at Georgetown University Law Center, with expected graduation in 2020. She is a Featured Online Contributor for Volume 56 of the *American Criminal Law Review.*

[1] *See* Florida v. Jardines, 569 U.S. 1, 6 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals").

[2] Silverman v. United States, 365 U.S. 505, 511 (1961).

[3] *See* Payton v. New York, 445 U.S. 573, 590 (1980) ("[T]he Fourth Amendment has drawn a firm line at the entrance to the house").

[4] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (noting that the Fourth Amendment does not protect "information revealed to a third party and conveyed by [the third party] to Government authorities, 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"); Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239, 1281 (2017).

[5] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[6] U.S. CONST. amend. IV.

[7] *See, e.g.*, Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo.

[8] *See, e.g., id.*

I. VOLUNTARINESS AND THE THIRD-PARTY DOCTRINE

Voluntary exposure is at the heart of the third-party doctrine.[9] Yet, this element of choice is shrinking in the face of technology. Justice Sotomayor called the doctrine "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties" as a matter of course.[10] More recently, in *Carpenter v. United States*, the Court declined to extend the third-party doctrine to cell-site location information, requiring the Government to obtain a warrant before searching those records.[11] The doctrine's underlying rationale – voluntary exposure – did not apply there, because carrying a cell phone is no longer a meaningful choice.[12] Rather, it is "indispensable to participation in modern society."[13]

The same will be true of the smart home. Around thirty-nine million Americans own smart home devices like Amazon's Echo, which features the voice assistant Alexa.[14] Nearly half of those owners say they are essential to daily life.[15] Alexa turns down the lights and warms the house.[16] She orders groceries and entertains the kids.[17] Soon, she will likely be in every home appliance, from ceiling fans to coffee makers to refrigerators.[18] The Alexa Connect Kit – Amazon's chip – can make anything smart (think an Alexa-powered toaster, or a microwave that

---

[9] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[10] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
[11] *Carpenter*, 138 S. Ct. at 2220.
[12] *Id.*
[13] *Id.*
[14] Kevin Murdane, *Report Claims That 16% Of Adults In The US Own Amazon's Echo Or Google's Home*, FORBES (Jan. 13, 2018, 8:00 AM), https://www.forbes.com/sites/kevinmurnane/2018/01/13/report-claims-that-16-of-adults-in-the-us-own-amazons-echo-or-googles-home/#7cf3fc078d88; *The Smart Audio Report*, N.P.R. AND EDISON RESEARCH, 3 (2017), https://nationalpublicmedia.com/wp-content/uploads/2017/06/The-Smart-Audio-Report-from-NPR-and-Edison-Research-2017.pdf.
[15] *The Smart Audio Report*, *supra* note 14, at 12.
[16] Brief for Technology Companies as Amici Curiae in Support of Neither Party at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
[17] *Id.*; *The Smart Audio Report*, *supra* note 14, at 11.
[18] Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. TIMES (Oct. 10, 2018), https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html (describing "the internet of things" – everyday objects set to become smart).

replenishes popcorn when stock is low).[19] At that point, the third-party doctrine will transform "the 'physical sanctity' of the home" into "an empty legal vessel."[20]

II. ALEXA AS A MURDER WITNESS

Alexa is always listening for her name, or another wake word.[21] When she hears it, she starts recording and sends the interaction to the Amazon cloud.[22] There is no limit to the use of this information. Timothy Verrill of New Hampshire is the latest defendant – charged with double murder – to confront this reality.[23] Verrill was not the owner of the residence where the bodies were found (and therefore not the owner of the Echo), but he knew the homeowner and had access to the security code.[24] A home surveillance video captured footage of Verrill with two women – one of whom was the homeowner's girlfriend – before police discovered their bodies in the backyard.[25] The court found that there was probable cause to believe the Alexa speaker could have been recording:

> [T]he State's motion to search in lieu of a search warrant is granted . . . The court directs Amazon.com to produce forthwith to the court any recordings made by an Echo smart speaker with Alexa voice command capability . . . from the period of January 27, 2017 to January 29, 2017, as well as any information identifying cellular devices that were paired to that smart speaker during that time period.[26]

Amazon maintains that it will not release recordings without a properly served, valid and binding legal demand.[27] It took a similar stance when an Arkansas court issued a search warrant for electronic data from

---

[19] *Id.*; Jon Bird, *A Slew of New Alexa Devices Expands Amazon's 'Echo-System'*, FORBES (Sept. 20, 2018, 10:33 PM), https://www.forbes.com/sites/jonbird1/2018/09/20/a-slew-of-new-alexa-devices-expands-amazons-echo-system/#622fcd396ae8.

[20] Joseph Jerome, *Alexa, is Law Enforcement Listening?*, CENTER FOR DEMOCRACY & TECHNOLOGY (Jan. 4, 2017), https://cdt.org/blog/alexa-is-law-enforcement-listening/.

[21] *Id.*; *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230.

[22] *Alexa Terms of Use*, AMAZON (May 17, 2018), https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740.

[23] Mark Osborne, *Judge Orders Amazon to Hand Over Echo Recordings in Double Murder Case*, ABC NEWS (Nov. 10, 2018, 2:29 AM), https://abcnews.go.com/US/judge-orders-amazon-hand-echo-recordings-double-murder/story?id=59100572.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

Amazon in another murder investigation.[28] Alexa was streaming music on the night in question, and law enforcement hoped she was accidentally triggered to record the events.[29] Amazon worried that handing over the records would chill users' First Amendment rights in their homes, and filed a motion to quash the warrant.[30] It stressed that the vast amount of information stored in Echo's digital records far exceeds that which can be gleaned from paper documents.[31] The point was rendered moot when the defendant and homeowner – James Bates – consented to the search.[32]

In the first case, it is unclear whether Verrill was permitted on the premises, and the extent of his relationship with the homeowner and victims. However, he certainly enjoyed a lesser expectation of privacy, if any.[33] Under the third-party doctrine, Bates, the homeowner in the second case, arguably had no better Fourth Amendment protections than Verrill. Despite the elevated status of the home under Fourth Amendment law, both defendants – the homeowner and the apparent trespasser – had the same privacy rights (none) in the Echo recordings. This troubling result is the very outcome that the Court in *Kyllo* tried to avoid: "[leaving] the homeowner at the mercy of advancing technology."[34] There, Justice Scalia worried that the Government might discover intimate details behind the four walls of the home, like when "the lady of the house takes her daily sauna and bath."[35] Now, Alexa is the one drawing her bath (at her preferred preset temperature, no less).[36] As Amazon said in *Bates*: "the lives of Americans may be racing ahead of existing court rulings."[37]

III. THE LOW BAR PROVIDED BY FEDERAL STATUTES

The Alexa searches from the Verrill and Bates cases were based on probable cause. In the future, though, the Government might argue that it

---

[28] *See* Arkansas v. Bates, No. CR20160370, 2016 WL 7587403 (Ark. Cir. Aug. 26, 2016).
[29] Adrienne N. Kitchen, *Smart Devices and Criminal Investigations: Protecting Suspects' Privacy and Fourth Amendment Rights*, 54 NO. 3 CRIM. LAW BULLETIN ART 1 (2018).
[30] *Id.*
[31] *Id.*
[32] Michael Harrigan, *Privacy versus Justice: Amazon's First Amendment Battle in the Cloud*, 45 W. ST. L. REV. 91 (2017).
[33] *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 91 (1998) (holding that even some people permitted on the premises do not have a reasonable expectation of privacy).
[34] Kyllo v. United States, 533 U.S. 27, 35, 40 (2001) (holding that the Government's use of a thermal imaging device to detect heat emanating from a home violated the Fourth Amendment).
[35] *Id.* at 38.
[36] KOHLER, https://www.us.kohler.com/us/smarthome/content/smarthome.htm (last visited Nov. 13, 2018) (introducing "the world's smartest bathroom" featuring Amazon Alexa built right in).
[37] Kitchen, *supra* note 29.

does not need probable cause to access this data.[38] Indeed, law enforcement in the Bates case obtained data from Bates's smart water meter without a warrant after prosecutors thought he may have used it to hose down blood.[39] Although federal statutes provide greater protection than the third-party doctrine, they set the bar lower than probable cause. To obtain electronic communication records under the Stored Communications Act, the Government need only show *reasonable grounds* to believe the records are relevant and material to an ongoing criminal investigation.[40] The same low standard applies to wire taps.[41] In *Carpenter*, the police obtained a court order to search the petitioner's cell-site records pursuant to the Stored Communications Act.[42] They showed reasonable grounds to believe that the records were relevant and material to a robbery investigation based on tips from a suspect, who identified accomplices and provided their cell phone numbers to the FBI.[43]

Chief Justice Roberts called the reasonable grounds standard "a 'gigantic' departure from the probable cause rule," holding that probable cause "is required in the rare case where a suspect has a legitimate privacy interest in records held by a third party."[44] Given the rapid evolution of smart home technology, it is hardly a rare case where such privacy interests in third party records exist. Smart home devices will soon become a practical necessity of modern life,[45] just like cell phones (if they are not already). Therefore, this data must be protected by robust federal statutes and a doctrine based upon the holding in *Carpenter*.

IV. ALEXA UNDER THE *KATZ* DOCTRINE

Even more, the third-party doctrine as applied to modern home technologies does not hold up under a simple *Katz* expectations analysis.[46] For Fourth Amendment protections to attach, a person must have a subjective expectation of privacy that society is prepared to recognize as reasonable.[47] This determination depends on a normative inquiry.[48] As Justice Gorsuch noted in *Carpenter*, "[p]eople often *do* reasonably expect that information they entrust to third parties . . . will be kept private."[49]

---

[38] *See* Stanley, *supra* note 7.
[39] *Id.*
[40] Stored Communications Act, 18 U.S.C. § 2703(d).
[41] 18 U.S.C. § 2511(2)(h)(i)(III).
[42] Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
[43] *Id.*
[44] *Id.* at 2221–22.
[45] Brief for Technology Companies as Amici Curiae in Support of Neither Party at 9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).
[46] Katz v. United States, 389 U.S. 347, 361 (1967).
[47] *Id.*
[48] Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).
[49] *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

For example, a family reported that its Amazon Echo recorded a private conversation in the home and sent it to a random contact.[50] Amazon said Alexa misinterpreted background noise as a command to send the message.[51] This accidental recording is not an isolated incident,[52] and the third-party doctrine would allow such evidence to be admitted under the legal fiction that it had been voluntarily conveyed. Yet, under a normative test, it is difficult to imagine that this family – although it welcomed Alexa into its home – had no expectation of privacy in that conversation. In the age of the smart home, simply checking a box to allow third parties access to certain information should not be enough to void all privacy rights.

CONCLUSION

The third-party doctrine originated from the idea that the law does not protect one who relays information to a trusted accomplice who later betrays him.[53] Alexa, though, is no ordinary friend. If she has not already, she will soon infiltrate the most intimate of spaces. The Court has declined to extend the third-party doctrine to data gathered by cell phones, recognizing their "immense storage capacity" and necessity to modern life.[54] Due to this necessity, the Court deemed the rationale behind the doctrine – the voluntary assumption of risk – inapplicable in that context.[55] Because the smart home will soon be no different, the third-party doctrine cannot allow the data it gathers to be insulated from a Fourth Amendment challenge. Even today, it cannot be squared with the reasoning of *Katz*. Many of us still have an expectation of privacy in information we convey to third parties, especially when *not* sharing such information is a difficult feat. Federal statutes should be enacted to protect the snippets of privacy captured by Amazon's Echo and similar devices, and *Carpenter*'s rationale must be extended to protect information they collect. Otherwise, our smart homes just might outsmart us.

---

[50] Eugene Kim, *Amazon Echo Secretly Recorded a Family's Conversation and Sent it to a Random Person on their Contact List*, CNBC (May 24, 2018, 4:54 PM), https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html.

[51] *Id*.

[52] *See, e.g.*, Stanley, *supra* note 7 ("devices like Echo will sometimes misinterpret sounds as their 'wake word' and record random snippets of conversation").

[53] United States v. White, 401 U.S. 745, 752 (1971).

[54] *Carpenter*, 138 S. Ct. at 2214; Riley v. California, 134 S. Ct. 2473, 2489, 2495 (2014).

[55] *Carpenter*, 138 S. Ct. at 2220 (reasoning that "in no meaningful sense does the [cell phone] user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements").