THESE WALLS *CAN* TALK! SECURING DIGITAL PRIVACY IN THE SMART HOME UNDER THE FOURTH AMENDMENT

STEFAN DUCICH[†]

ABSTRACT

Privacy law in the United States has not kept pace with the realities of technological development, nor the growing reliance on the Internet of Things (IoT). As of now, the law has not adequately secured the "smart" home from intrusion by the state, and the Supreme Court further eroded digital privacy by conflating the common law concepts of trespass and exclusion in United States v. Jones. *This article argues that the Court must correct this misstep by explicitly recognizing the method by which the Founding Fathers sought to "secure" houses and effects under the Fourth Amendment. Namely, the Court must reject its overly narrow trespass approach in lieu of the more appropriate right to exclude. This will better account for twenty-first century surveillance capabilities and properly constrain the state. Moreover, an exclusion framework will bolster the reasonable expectation of digital privacy by presuming an objective unreasonableness in any warrantless penetration by the state into the smart home.*

INTRODUCTION

During Apple's Macworld keynote in January 2007, Steve Jobs unveiled "an iPod, a phone, and an Internet communicator," promising: "This will change everything."[1] Indeed, as the paragon of so-called 'smart' technology, the iPhone has changed entire industries, and in short order, introduced society at-large to an interconnected world.[2] This

---

[†] Stefan Ducich graduated *cum laude* from American University Washington College of Law in May 2017 and is barred in New York state. He specializes in the intersection of technology and privacy law, and currently works as a contract attorney in the Privacy Office of the Pension Benefit Guaranty Corporation on issues related to information security, breach response, and federal privacy law compliance. (The views expressed in this article are the author's own and do not represent those of PBGC.)

[1] Lisa Eadicicco, *Watch Steve Jobs Unveil the First iPhone 10 Years Ago Today*, TIME (Jan. 9, 2017), http://time.com/4628515/steve-jobs-iphone-launch-keynote-2007/.

[2] *See* SAMUEL GREENGARD, THE INTERNET OF THINGS xii (2016) (noting that the introduction of the iPhone on the market, and its impact on the market, was a

concept is increasingly – and quite literally – being brought home.[3] Network- and inter-connected devices, also referred to as the Internet of Things ("IoT"), are creating a "nervous system" within what is traditionally one of the most private of spaces: the home. Access "the house's digital hub and you can actually spy on [its] chattering stuff."[4]

Privacy law in the United States has not adequately kept pace with these technological developments, and its failure to recognize the unique character of digital information is undermining the security of the home against government intrusion. With the rejuvenation of a trespass-based conception of the Fourth Amendment in *United States v. Jones*,[5] the Supreme Court eroded digital privacy by relying on a legal concept better suited to the physical context.[6] Such reliance leads to perverse results. For example, one district court judge equated the FBI gaining remote access to a private computer by exploiting digital vulnerabilities (i.e., hacking) to an officer peering through a gap in an apartment's window blinds, and therefore not requiring a warrant.[7] By relying on this inappropriate analogy, the judge sanctioned full, unrestricted access to the data stored on a private computer without any showing of probable cause.

As of now, the legal landscape is not equipped to adequately protect against digital abuses by the state. Though a majority of the sitting members of the Supreme Court has signaled a willingness to accommodate

---

"crystalizing event" in the development of smart objects); *cf. Planet of the Phones*, THE ECONOMIST (Feb. 26, 2015), http://www.economist.com/news/leaders/21645180-smartphone-ubiquitous-addictive-and-transformative-planet-phones (noting that the "iPhone exemplifies the early 21st century's defining technology," its transformative power derived from its "size and connectivity").

[3] *See There's No Place Like [a Connected] Home*, MCKINSEY & CO., http://www.mckinsey.com/spContent/connected_homes/index.html (last visited Apr. 24, 2017) (demonstrating a thirty-one percent compound annual growth rate of connected homes from 2015 through 2017); *see also* Eric Griffith & Alex Colon, *The Best Smart Home Devices of 2018*, PC MAG (Dec. 1, 2017, 11:51 AM), http://www.pcmag.com/article2/0,2817,2410889,00.asp.

[4] Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013, 6:30 AM), https://www.wired.com/2013/05/internet-of-things-2/; *see generally, e.g.*, Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905 (2010) (detailing the "ideal of the inviolate home" in Fourth Amendment jurisprudence as a sphere afforded particular constitutional protection).

[5] 565 U.S. 400 (2012) (holding the attachment and subsequent use of a tracking device on a vehicle constitutes a trespassory interference with an "effect," and is therefore a search within the meaning of the Fourth Amendment).

[6] *Id.* at 404 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information.").

[7] United States v. Matish, 193 F.Supp. 3d 585, 615 (E.D. Va. June 23, 2016).

technological evolution into Fourth Amendment jurisprudence, the Court has yet to correct its misstep in *Jones*.[8] It must do so.

As noted in Part I of this paper, smart devices are prolific, and they create vulnerabilities in the security of the home. This section presents the Court's evolution on privacy protections from a property- to personhood-based paradigm. Thereafter, Part II clarifies that the Fourth Amendment has historically been linked to privacy rights as a means of articulating the security of, among other things, "houses . . . and effects"[9] from government intrusion. Part II then argues that a privacy-protective interpretation of the Fourth Amendment should be based on exclusion, rather than trespass. Thus, this paper concludes that the Court must reject *Jones*' overly-narrow trespass approach, problematic for the non-physical intrusion at issue with IoT, in lieu of the more appropriate right to exclude. An exclusion-based framework will better account for twenty-first century technological surveillance techniques. Doing so will fulfill the guarantees of the Fourth Amendment and ensure that the government may not unreasonably intrude upon digital privacy.

I. BACKGROUND

A. The Internet of Things Comes Home

Many associate smart devices with objects like Amazon's Echo, the speaker that connects users to its smart assistant, Alexa.[10] Yet beyond this, smart objects in the home are vast and varied. From the mundane to the extremely personal, from juicers to condoms,[11] the market share for

---

[8] *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (writing for the Court, Chief Justice Roberts noted that the search of a smartphone, with its vast quantity of information, "bears little resemblance to the type of brief physical search considered" in prior Fourth Amendment cases); Jones, 565 U.S. at 417 (Sotomayor, J., concurring) ("[T]he same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations."); Jones, 565 U.S. at 419 (Alito, J., concurring) (arguing for a review of reasonable expectations of privacy based on new surveillance capabilities, joined by Justices Ginsburg, Breyer, and Kagan).

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

[10] *See Alexa Voice Service*, AMAZON, https://developer.amazon.com/alexa-voice-service (last visited Dec. 13, 2017); Dan Eavon, *What is Alexa? It's Amazon's New Virtual Assistant*, DIGITAL TRENDS (Sept. 7, 2017, 1:03 PM), https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/.

[11] *See* Jeff Dunn, *17 Ridiculous 'Smart' Gadgets that Really Exist*, BUS. INSIDER (Mar. 14, 2017, 1:44 PM), http://www.businessinsider.com/weirdest-smart-gadgets-internet-of-things-smart-home-2017-3/#hidrate-spark-2; Griffith & Colon, *supra* note 3.

smart objects is growing.[12] To be sure, "connected devices are disrupting every nook of the home."[13] But what are the "things" in the IoT,[14] and what vulnerabilities are created by their proliferation?

Stated simply, IoT refers to a web of identifiable devices—the things—which are capable of automatically communicating data about the device to a system able to read and interpret that information.[15] Sensors are embedded in otherwise "dumb" objects to sense the environment around them and communicate that information onward.[16] Not all smart devices are connected to the Internet in the strictest sense, though they may use the same Internet Protocol; indeed, some "smart" objects are so categorized because they contain a simple sensor like a radio frequency identification ("RFID") chip that "talks" to some central system.[17]

---

[12] *See* MCKINSEY & CO., *supra* note 3 (detailing the current market for smart-devices objects, current obstacles, and potential for growth); *see also* Peter M. Lefkowitz, *Making Sense of the Internet of Things*, 59 BOS. B.J. 23, 23 (Fall 2015) ("[IoT] will have an annual economic impact of between $4 trillion and $11 trillion by 2025.").

[13] MCKINSEY & CO., *supra* note 3 (listing "home intelligence, energy efficiency, entertainment, wellness, access control, home safety, home comfort, daily tasks, [and] connectivity").

[14] To succinctly articulate the privacy issues inherent with IoT devices, this paper's scope is limited to smart objects inside the home. Under the current doctrinal construction of the Fourth Amendment, the location of activity complicates the analysis. *See generally Overview of the Fourth Amendment*, 45 GEO. L.J. ANN. REV. CRIM. PROC. 3 (2016). For instance, more nuance is needed for devices that are carried by a person both inside and outside the home (i.e., FitBit) and for objects that are just as likely to be in a home as in a location where the presumption of privacy has been found to be reduced (i.e., smart televisions in schools). *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 655 (1995) (holding a diminished expectation of privacy in schools). While the character of the data that is collected by such devices is similar in kind to that collected in the home—and is therefore also worthy of privacy protections argued for in this paper—for rhetorical clarity, the smart devices at issue here are limited to those found within a home.

[15] *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 823–24 (2016) ("Some definitions of IoT would require a higher level of interoperability to qualify as being part of the IoT.").

[16] Michael Chui, et al., *The Internet of Things*, MCKINSEY Q. (Mar. 2010), http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things.

[17] *See id*.; INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, FED. TRADE COMM. 5 (Jan. 2015) [Hereinafter FTC STAFF REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-

The point of all IoT devices, however, is to gather information: "[T]hese networks churn out huge volumes of data that flow to computers for analysis . . . . They become tools for understanding complexity and responding to it swiftly."[18] Fundamentally, the IoT is a system of gathering large quantities of information that amount to private surveillance of the user's activities, preferences, and habits in the home.[19] This information is then "leveraged" to optimize the function of the given object.[20] Though primitive smart objects were initially designed to improve manufacturing,[21] today "these connected devices . . . collect, transmit, store, and potentially share vast amounts of [highly personal] consumer data."[22] This information is granular in detail and almost incomprehensibly large in quantity.[23]

To the extent that "internet connectivity makes good objects great," it appears that "a chip-centric mentality has taken over," without necessarily accounting for the security of the home network.[24] Not all smart objects are designed with the same level of intelligence, or with the

---

privacy/150127iotrpt.pdf (discussing the continued ambiguity in IoT's definition); *cf.* Matt Burgess, *What is the Internet of Things?, WIRED Explains*, WIRED UK (Apr. 21, 2017), http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot (distinguishing from "simple sensors" to "smartphones and wearables").

[18] Chui, et al., *supra* note 16; *see* Patrick McFadin, *Internet of Things: Where Does the Data Go?*, WIRED, https://www.wired.com/insights/2015/03/internet-things-data-go/ (last visited Apr. 26, 2017).

[19] Ferguson, *supra* note 15, at 818–19; *see* Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14, 15 (2016) (quoting the head of regulatory affairs at Siemens Metering Systems, saying "we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data").

[20] Daniel Burrus, *The Internet of Things is Far Bigger than Anyone Realizes*, WIRED, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ (last visited Apr. 25, 2017).

[21] Robin Kester, *Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations*, 8 ELON L. REV. 205, 206 (2016).

[22] FTC STAFF REPORT, *supra* note 17, at 2.

[23] *See* Alex Wall, *Privacy and the Internet of Things: Everything Around You is Collecting your Private Data*, RADAR (Oct. 21, 2016), https://www.radarfirst.com/blog/privacy-and-the-internet-of-things ("By 2020, the Internet of Things will comprise no less than 50 billion devices and 212 billion sensors, generating 44 zettabytes of information. A zettabyte is 10^{21} bytes or 1,000,000,000,000,000,000,000.").

[24] Woodrow Hartzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & TECH. 581, 583 (2016).

long-term functionality of the device in mind; think, for instance, about the average lifespan of a refrigerator versus a shampoo bottle, both of which are now connected "things."[25] A smart device only functions as such so long as its software is up-to-date.[26] On one hand, some of these devices may be used in the home well beyond the point where the manufacturer—now a service provider—continues to patch critical vulnerabilities.[27] Conversely, some devices are designed to be quickly disposed of, so they are not serviced at all due to the limited capacity of the object's bandwidth or RFID.[28] Yet, all software is a potential access point, a vector through which the security of a network may be compromised.[29]

Left unchecked, smart objects potentially can be transformed into tools of invasive surveillance by the state.[30] Malicious (i.e., black hat) hackers already have proven that IoT devices are prime targets for infiltration:[31] anecdotal stories proliferate, with hackers yelling at children through digital baby monitors[32] and experiments proving the "inevitability" of an unsecured toaster being breached once connected to

---

[25] *Id.* at 586–87 ("Security researcher Brian Krebs notes that poorly configured default settings for IoT devices are a security nightmare. This is particularly true for devices that are costly to change, like many disposable ad cheap IoT devices.").

[26] *Id.* at 583–84 (noting that software can crash suddenly and needs updates and upgrades to maintain its connectivity).

[27] *See id.* at 588–89 ("The typical lifetime of software is around 2 years. But the estimated lifetime of some objects now connected to the Internet is often around 10 years. Just think about how long coffee pots and refrigerators last.").

[28] *Id.* at 586.

[29] *See e.g.*, Nick Ismail, *The Internet of Things: The security Crisis of 2018?*, INFO. AGE (Jan. 22, 2018), http://www.information-age.com/internet-things-security-crisis-123470475/ ("The influx of additional entry points… plus a current lack of security standards for IoT devices, means there is a gaping hole in the perimeter of any home… that has installed IoT devices."); *see also* Hartzog & Selinger, *supra* note 24, at 588 (noting that "every new IoT connection brings new risks").

[30] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1013 (2016) (comparing the potential for invasive surveillance of private spheres via IoT to that of CCTV in public).

[31] Kim Zetter, *Hacker Lexicon: What are White Hat, Gray Hat, and Black Hat Hackers?*, WIRED (Apr. 13, 2016, 5:03 PM), https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers ("Black hats are criminals. They use their prowess to find or develop software holes and attack methods.").

[32] Kashmir Hill, *The Half-Baked Security of Our 'Internet of Things'*, FORBES (May 27, 2014, 2:56 PM), https://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/.

the Internet.[33] Governments are undeniably able, and they in fact are engaged in hacking;[34] indeed, Congress has made it easier for U.S. law enforcement to remotely access computing devices for investigatory purposes.[35] Like the black hats above, law enforcement agencies are working to develop, and in some cases already possess, the capabilities to access not only traditional computing devices but also smart objects within the home.[36] To wit, the depth and scope of knowledge available to the government, should it seek to gain access to the smart-home's "nervous system," is exactly the type of intrusion the Fourth Amendment was designed to secure against.[37]

B. The Fourth Amendment

The Fourth Amendment declares inviolate "the right of the people to be secure in their persons, houses, papers, and effects."[38] It protects against unreasonable government intrusions by establishing a certain right to privacy enforceable by the individual "as against the world."[39] Yet, the Amendment is not clear as to exactly how this is manifested. Supreme Court jurisprudence on this point has vacillated between a purely property

---

[33] Andrew McGill, *The Inevitability of Being Hacked*, THE ATLANTIC (Oct. 28, 2016), https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/.

[34] Eva Galperin, *The Year in Government Hacking: 2016 in Review*, ELEC. FRONTIER FOUND. (Dec. 26, 2016), https://www.eff.org/deeplinks/2016/12/year-government-hacking.

[35] *See* FED. R. CIV. P. 41; *Supreme Court Approves Change to Rule 41 Search and Seizure Warrants for Electronic Property*, THE NAT'L SEC. L. BRIEF (Apr. 29, 2016), http://nationalsecuritylawbrief.com/supreme-courts-approves-change-to-rule-41-search-and-seizure-warrants-for-electronic-property/; Kate Tummarello, *The Fight Over Government Hacking Continues*, ELEC. FRONTIER FOUND. (Dec. 6, 2016), https://www.eff.org/deeplinks/2016/12/fight-over-government-hacking-continues; *see also* Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, 'Particularly' Speaking*, 51 U. RICH. L. REV. 272 (2017) (arguing for the propriety of the 2016 Amendments to Rule 41).

[36] *See Vault 7: CIA Hacking Tools Revealed*, WIKILEAKS, https://wikileaks.org/ciav7p1/ (last visited Apr. 24, 2017); *see also* David Choi, *WikiLeaks Publishes More Secret CIA Tools After the US Threatens Criminal Charges*, BUS. INSIDER (Apr. 21, 2017), http://www.businessinsider.com/wikileaks-cia-hacking-tools-samsung-weeping-angel-2017-4 (detailing the "Weeping Angel" tool that activates Samsung televisions' built-in microphones for surveillance purposes).

[37] *See* Ferguson, *supra* note 15, at 820 (explaining that a "data-rich environment creates a wider mosaic of life patterns," allowing police to virtually and constantly surveil).

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

[39] *See id.*; Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213. (Dec. 15, 1890).

(*in rem*) conception,[40] to one based on expectations of privacy (*in personam*),[41] to a hybrid of the two.[42] As a result, the current Fourth Amendment framework imperils the security of digital information emanating from the home; it fails to accommodate the scope of the right the framers intended to protect and ignores how they sought to do so.

The Amendment does not protect privacy as such. Rather, it identifies and guarantees enumerated property interests, thus buttressing a sphere within which the intimacies of life may be protected.[43] Until the mid-twentieth century, property law dominated the Court's jurisprudence and increasingly obscured the underlying privacy interest.[44] For instance, the Court's 1886 decision in *Boyd v. United States*[45] solidified the subordinate relationship of privacy to property, where intrusion upon the latter established the harm to the former. "Every invasion of private property," the *Boyd* Court declared, "be it ever so minute, is a trespass."[46] *Boyd* subsumed privacy under the harm to property, thus triggering a constitutionally protected interest.[47] The *Boyd* Court was also at pains to point out that "the eye cannot by the [common law] be guilty of a

---

[40] *See, e.g.*, Olmstead v. United States, 277 U.S. 493 (1928) (holding search and seizure are dependent upon physical interference with tangible effects).

[41] *See* Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) ("[A] person has a reasonable expectation of privacy," particularly in the home, and "the invasion of a constitutionally protected area by federal authorities is . . . presumptively unreasonable in the absence of a search warrant"); *see also* Kyllo v. United States, 533 U.S. 27, 31 (2001) (reaffirming the reasonable expectation of privacy as the basis of Fourth Amendment protections).

[42] *See* United States v. Jones, 565 U.S. 400, 406 (2011) (reasserting trespass as a controlling factor in defining an unreasonable search, separate and complimentary to the *Katz*-based reasonable expectation of privacy).

[43] *See* Ricardo J. Bascuas, *Property and Probable Cause: The Fourth Amendment's Principled Protection of Privacy*, 60 RUTGERS L. REV. 575, 622–23 (2008) (labeling "privacy" as the underlying interest protected through the security of property); *see also* William Clark, Note, *Protecting the Privacies of Digital Life:* Riley v. California, *The Fourth Amendment's Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1988 (2015) (quoting *Boyd*, and detailing "privacies" as the intimate details of a person's life).

[44] *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 312 (1998) (starting from the late eighteenth century, with *Boyd*, through the latter half of the twentieth century "the Supreme Court defined the interest secured by the Fourth Amendment largely in terms of property rights").

[45] 116 U.S. 616 (1886).

[46] *Id.* at 627.

[47] *See id.* at 628 (noting that a violation of the "secret nature of [private papers] will be an aggravation of the trespass").

trespass."[48] Pursuant to this theory, observation alone is insufficient; rather, some physical interference with the property named in the Amendment is necessary before privacy may be infringed.

This fealty to property is increasingly at odds with individual privacy as society develops its technological savvy. One of the earliest instances of this growing disconnect came in 1928, when the Court decided *Olmstead v. United States*.[49] That case concerned the admissibility of evidence obtained pursuant to a warrantless wiretap, which in turn proved a criminal bootleg conspiracy.[50] The *Olmstead* Court focused on where the wiretapping occurred, noting that it was done "without trespass upon any property of the defendants" since the wires were physically located in public spaces.[51] As such, the Court concluded that law enforcement's eavesdropping on telecommunications did not violate the Fourth Amendment because no property interest was infringed.[52] Consequently, the Court failed to protect the privacy of information that originated, at least partially, from within the home, an otherwise protected space within the plain text of the Fourth Amendment. The Court had difficulty identifying any privacy right separate from the tangible objects listed in the Amendment.[53] It rejected outright the notion that protection could extend to "telephone wires, reaching to the whole world," since they were not within any defendant's house or otherwise directly associated with their private property.[54]

With *Silverman v. United States*,[55] decided in 1961, the Court declined to revisit its *Olmstead* logic to account for technological advancements in the intervening years. There, when confronted with the use of a "spike mike," the Court declined to go beyond the trespass analysis.[56] Ignoring any conception of privacy separate from an invasion of property, the Court declared "a fair reading of the record in this case shows that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by the

---

[48] *Id.* at 628.
[49] 277 U.S. 438 (1928).
[50] *Id.* at 455.
[51] *Id.* at 457.
[52] *Id.* at 466 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").
[53] *Id.* at 464 ("The amendment itself shows that the search is to be of material things.").
[54] *Id.* at 465.
[55] 365 U.S. 505 (1961).
[56] *Id.* at 506 (clarifying that "[t]he instrument in question was a microphone with a spike about a foot long attached to it," which was inserted through a vacant room into an adjoining row house where it made contact with heating duct that amplified the mic's capabilities).

petitioners."[57] While the Court found that Silverman's rights had been violated, it did so based on the state's intrusion into the building's heating duct, not on any notion of personal privacy owed to Silverman, distinct from his property interest.[58]

This trespass-dependent equation broke down completely in 1967 as the Court shifted from an *in rem*, property-based right to an *in personam*, privacy-based paradigm.[59] In *Katz v. United States*,[60] the Court found that the Fourth Amendment's protections "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[61] For the first time, the Court rejected the notion that the Fourth Amendment was limited to "a given 'area,' viewed in the abstract, [as] 'constitutionally protected.'"[62] Rather, the rights ensured by the Amendment vest in "people, not places."[63] While the Court's *in personam* reasoning was a monumental shift, the enduring legacy of *Katz* comes from Justice Harlan's famous concurrence. Following *Katz*, Fourth Amendment privacy protections are based upon reasonableness: where a subjective expectation of privacy exhibited by the individual is found objectively reasonable by society.[64]

Notably, the Court did not reject the notion that particular locations are secured as such, by virtue of their character.[65] Rather, it uncoupled trespass as a pre-requisite to privacy intrusions, allowing the right to vest directly in the individual.[66] Certain areas are still very much at the fore of the Court's thinking when evaluating constitutional

---

[57] *Id.*

[58] *Id.* at 509 ("Eavesdropping accomplished by means of such a physical intrusion is beyond the pale.").

[59] Jace C. Gatewood, *The Evolution of the Right to Exclude – More than a Property Right, a Privacy Right*, 32 MISS. C. L. REV. 447, 457–58 (2014).

[60] 389 U.S. 347 (1967).

[61] *Id.* at 353.

[62] *Id.* at 352.

[63] *Id.*

[64] *See id.* at 361 (Harlan, J., concurring) (finding a twofold requirement to establish a reasonable expectation of privacy); *see also* United States v. Jones, 565 U.S. 400, 408 (2012) (reaffirming the expectation of privacy standard); Kyllo v. United States, 533 U.S. 27, 44 (2001) (basing its analysis upon the two-part reasonableness standard).

[65] *See, e.g.*, Oliver v. United States 466 U.S. 170, 176 (1984) (quoting Hester v. United States, 265 U.S. 57, 59 (1924) ("[The] Amendment indicates with some precision the places and things encompassed by its protections. . . . 'The distinction between [open fields] and the house is as old as the common law.'").

[66] *See* Katz, 389 U.S. at 352 (noting that to read the Fourth Amendment exclusively through the lens of a property-based right "is to ignore the vital role" that pervasive technologies play in modern life).

protection—the home being chief among them, as an expressly protected object under the Amendment.[67]

Following *Katz*, the Fourth Amendment secures two aspects of privacy, in equal measure. First, *in personam*, reasonable expectations of privacy are protected. Second, certain locales are singled out for specific protection. The Court, however, continues to grapple with the issue of technological invasions of the home.[68] In deciding these cases, the Court has relied both on the constitutional sanctity of the home and on expectations of privacy, but it has yet to properly balance digital privacy interests.

In *Kyllo v. United States*,[69] in 2001, the Court addressed "[the] power of technology to shrink the realm of guaranteed privacy."[70] The case concerned the warrantless use of thermal imaging of Danny Lee Kyllo's home by law enforcement agents, who deployed a heat-sensing device to detect the presence of high-intensity lamps for growing marijuana indoors.[71] The scan, conducted from across the street, identified a single room that was relatively hotter, thus tending to prove the presence of such lamps.[72] In 1992, when the scan was completed, mobile thermal technology of the kind used against the Kyllo residence was not in widespread use, which factored heavily in the decision by the Court.[73] Writing for the majority, Justice Scalia declared that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where . . . the technology in question is not in general public use."[74] The *Kyllo* Court was keen to maintain flexibility in its interpretation of the Fourth

---

[67] *See* U.S. CONST. amend. IV (protecting houses directly); *see also* Stern, *supra* note 4, at 913 ("In a jurisprudence focused on privacy versus publicity, the home is the quintessential private space.").

[68] *Cf.* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017) (surveying privacy jurisprudence relating to electronic surveillance in public, with reflections of the law relating to the home).

[69] 533 U.S. 27 (2001).

[70] *Id.* at 34 (addressing how much technological enhancement is too much to survive constitutional scrutiny).

[71] *Id.* at 30.

[72] *Id.*

[73] *See id.* at 30, 40.

[74] *Id.* at 34 (internal quotation and citation omitted).

Amendment to preserve protection against "technology that could discern all human activity in the home."[75]

In 2012, however, by declaring that trespass was again determinative in *United States v. Jones*, the Court upended the trajectory of its Fourth Amendment decisions, which theretofore had progressed towards a more digital privacy-protective framework.[76] In doing so, it introduced a hybrid *in rem*/*in personam* interpretation of the Amendment. *Jones* concerned the pervasive surveillance of a vehicle—an "effect" within the meaning of the Fourth Amendment[77]—through the attachment of a GPS tracker without a valid warrant.[78] Despite the Court's exclusive reliance on expectations of privacy since *Katz* in 1967, Justice Scalia, again writing for the majority, reiterated that the Court's privacy jurisprudence "embod[ies] a particular concern for government trespass."[79] He reasoned that, at a minimum, the Amendment's guarantee against unreasonable searches must replicate "the degree of protection it afforded when it was adopted."[80] Thus, he found that law enforcement had trespassed against Jones' constitutionally protected "effect;" as such, no further privacy analysis was necessary.[81] As a result, per Justice Alito's concurrence, the majority opinion relies on "18th-century tort law" to address a "21st-century surveillance technique."[82] The Court assures, however, that had no interference with property occurred, the reasonable expectation of privacy would control.[83]

By re-animating trespass as a legitimate basis for Fourth Amendment protections, the *Jones* Court recalled into existence the historic requirement for "a physical intrusion . . . by the government on property belonging to another,"[84] as in the *Boyd-Olmstead-Silverman* line

---

[75] *Id.* at 35–36 (indicating in dicta that such surveillance may have constitutional implications).
[76] *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("Jones' Fourth Amendment Rights do not rise or fall with the *Katz* formulation.").
[77] *See* Oliver v. United States 466 U.S. 170, 177 n.7 (1984) (noting that the framers would label personal, rather than real property as an "effect"); Ferguson, *supra* note 15, at 828 (noting "effects" within the meaning of the amendment generally refers to goods, moveable objects, or possessions: an individual's personal property).
[78] Jones, 565 U.S. at 404 (defining a vehicle as a Fourth Amendment effect, and the attachment thereto of a GPS tracking device to be a trespassory search).
[79] *Id.* at 406.
[80] *Id.* at 411.
[81] *Id.* at 412–13.
[82] *Id.* at 418 (Alito, J., concurring).
[83] *Id*. at 411 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.") (emphasis removed).
[84] Gatewood, *supra* note 59, at 454.

of cases. Indeed, trespass at common law has a specific meaning: as narrowly defined by Sir William Blackstone, trespass "signifie[d] no more than an entry on another man's ground without a lawful authority, and doing some damage, however inconsiderable."[85] In turning to this particular conception of property rights at common law, the *Jones* Court side-stepped another central property right, arguably the *sine qua non*: the right to exclude.[86] Per Blackstone, property is "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[87]

Indeed, *Jones* leaves open several lingering questions about how the Fourth Amendment protects and secures digital privacy in the age of the IoT. The Court's evolution from its exclusive dependence in *Boyd*, *Olmstead*, and *Silverman* on *in rem*, and specifically trespassory, harm, gave way to a right vested directly in the person.[88] The reasonable expectation of privacy recognized for the first time the tangible and intangible aspects of the privacy right secured by the Fourth Amendment, by vesting *in personam*. *Katz* therefore distinguished the personhood and property form of the right, while continuing to recognize certain specific locations whose protection remains heightened.[89] *Kyllo* is a prime example where the *in rem* right yielded to the *in personam*, with the Court finding it unreasonable to expect certain surveillance technologies being deployed against a home.[90] *Kyllo* left open the question of reasonable expectations regarding commonly used technologies,[91] but *Jones* radically altered the trajectory of the Court's jurisprudence by recalling into force the trespass analysis—abandoned a half-century before—as the controlling framework.[92] This last turn in the Court's jurisprudence leaves digital privacy open to abuse by the state, where strict interpretations of

---

[85] WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 3, at 209 (photo. Reprint, Univ. of Chi. Press 1979) (1766).
[86] *See* Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) (explaining the logical and historical primacy of the right to exclude in property law).
[87] *Id.* at 734 (quoting WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 2, at 2 (photo. Reprint, Univ. of Chi. Press 1979) (1766).
[88] *See* Gatewood, *supra* note 59 at 457–58 (discussing the evolution from a property-based to a privacy-based paradigm).
[89] *Id.* at 461.
[90] *See* Kyllo v. United States, 533 U.S. 34 (2001).
[91] Cf. *id*. (basing its holding on the lack of common usage).
[92] *See* Ferguson, *supra* note 15, at 832 (concluding that, among other things, *Jones* resurrected the "long-dormant" trespass theory of the amendment).

property rights overwhelm reasonable expectations of privacy, or where courts are unwilling to find an objective expectation of reasonableness.[93]

II. ANALYSIS

New technologies fundamentally alter society.[94] Still, the durability of constitutional protections depends upon the law accommodating how people interact with these new technologies and how law enforcement may legitimately utilize the benefits of technological development.[95] The essence of the Fourth Amendment, however, is to restrain unwarranted government action against the individual: it is the expression of the framers' intent to secure the American people from intrusion by the state, in the form of unreasonable search and seizure.[96] Without a proper recognition by the Court of how the Fourth Amendment protects digital privacy, virtual access by law enforcement threatens the security of citizens in their houses and digital effects.[97] Thus, to ensure privacy in the face of evolving technology, it is once again "necessary . . . to define anew the exact nature and extent of such protection."[98]

In a world dominated by smart devices, the right to exclude—not trespass—is the better analytical framework. As clarified below, the use of property rights by the framers was not so literal; it was a method of articulating privacy rights "secured" under the Fourth Amendment. Indeed, the state is precluded from exploiting digital vulnerabilities in the home unless it overcomes the burdens imposed on it by the Fourth Amendment to prove reasonableness.[99] Yet, the analysis (re)instituted by *Jones* in 2012 does not adequately account for the data-rich environment created by smart devices in the home, or the wide-ranging surveillance

---

[93] *Cf.* United States v. Jones, 565 U.S. 414, 425–26 (2012) (Sotomayor and Alito, JJ., concurring) (noting lingering issues unaddressed by the purely trespass theory of the majority).

[94] *See, e.g.*, Jim Luce, *The Impact of Cell Phones on Psychology, Community, Culture, Arts and Economics*, Huffington Post (May 25, 2011), http://www.huffingtonpost.com/jim-luce/the-impact-of-cell-phones_b_508011.html (discussing smart phones' impact on the quality of people's lives).

[95] *Cf.* Gatewood, *supra* note 59, at 457–58 (recognizing action by the Court in response to developing technologies to ensure proper privacy protections in its adoption of the Katz standard).

[96] *See* Weeks v. United States, 232 U.S. 383, 390 (1914).

[97] *See* U.S. Const. amend IV; Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143, 161 (2015).

[98] Warren & Brandeis, *supra* note 39, at 193.

[99] *See* Ferguson, *supra* note 15, at 822

opportunities they afford to law enforcement.[100] Rather, the Court should build on its decision in *Kyllo* to strengthen the *in personam* expectation of privacy by making explicit its reliance on exclusion as a means of perfecting the Fourth Amendment's "security."[101] Doing so will properly constrain the state's ability to gain access to the digital home.

A. The Fourth Amendment is a Means of "Securing" Privacy

The founding fathers were pragmatic in their use of property rights at common law to express the scope of the Fourth Amendment, but their intent to protect a right to privacy vested in the person is clear by the term used to conserve such rights: namely, to "secure." In crafting the Fourth Amendment, the framers were determined to guarantee safeguards that would prohibit "invasions of the home and [thereby, to secure] privacy of the citizens."[102] In essence, resistance to unreasonable search and seizure was the codification of the maxim: "a man's house [is] his castle . . . not to be invaded by any general authority."[103] Thus, the Amendment's drafters sought to protect "the sanctity of a man's home and the privacies of life" through property law as a means of guaranteeing that sphere of protection.[104]

Property law is "deployed as a means of operationalizing privacy, not replacing it."[105] The enumeration of certain tangible objects—persons, houses, papers, and effects—was meant to cover the breadth of personal interests guaranteed by the Fourth Amendment.[106] Rather than elevate tortious trespass by the government to the level of constitutional protection, these property rights articulate the scope of the privacy right.[107] As such, these objects represent the sphere within which "the privacies of life" are protected.

---

[100] *See id.* at 818–19; *see also* United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) (presenting the "mosaic theory" whereby largescale, aggregated data reveals the intimacies of life).

[101] *See* section II.c *infra* (arguing for the replacement of trespass with exclusion as a means of establishing a reasonable expectation of digital privacy).

[102] Weeks v. United States, 232 U.S. 383, 389–390 (1914); *see* Clancy, *supra* note 44 at 310.

[103] Weeks, 232 U.S. at 390.

[104] Boyd, 116 U.S. at 603 (referencing *Entick v. Carrington*, 19 Howell's State Trials 1029, 95 Eng. Rep. 807 (C.P. 1765) as evidence of the founding fathers' purpose in crafting the Fourth Amendment).

[105] Slobogin, *supra* note 97, at 156.

[106] *Id.*; *see also* Boyd, 116 U.S. at 630.

[107] *See* Bascuas, *supra* note 43, at 622.

Thus, property is the means to explain the scope of the constitutional privacy right,[108] and security is the action effectuating the Fourth Amendment's purpose.[109] Indeed, the Fourth Amendment speaks explicitly of a right to be "secure" in the enumerated property interests.[110] For the framers, "security" from unreasonable intrusion referred to the right to exclude; to wit, it is the essential attribute of the action guaranteed by the Amendment.[111] "Without the ability to exclude, a person has no security. With the ability to exclude, a person has all the Fourth Amendment promises: protection against unjustified intrusions by the government."[112]

This right to exclude extends to all private property, both real and personal, guaranteed through the Fourth Amendment's enumeration of tangible objects—the text of the Amendment does not draw hierarchies between houses and effects. As Samuel Warren and Louis Brandeis noted in their seminal work on the right to privacy, "the term 'property' has grown to comprise every form of possession—intangible, as well as tangible."[113] As such, the ability to exclude proscribes all unreasonable intrusion by the state, tangible and intangible.[114]

The right to exclude is fundamental to property at common law—related, but distinct from the narrower trespass.[115] The Fourth Amendment is not concerned with tortious trespass, as Justice Scalia's opinion in *Jones* asserts. Rather, the Amendment excludes the government from specific objects as a means of articulating the breadth of a constitutional right to privacy. This distinction is necessary in a modern context where virtual intrusion by law enforcement threatens the security of the smart home. "Security" through exclusion guarantees the inviolability of both the tangible and intangible effects protected by the Fourth Amendment and therefore is the most appropriate framework given the advent of IoT.[116]

---

[108] *Id.* at 622–23 ("'Property' for Fourth Amendment purposes needs to be interpreted to further the underlying purpose of protecting privacy.").
[109] *See generally*, Clancy, *supra* note 44 (articulating security as the function of the Fourth Amendment).
[110] *See* U.S. Const. amend. IV; *see also* Ferguson, *supra* note 15, at 861.
[111] *See* Clancy, *supra* note 44, at 308.
[112] *Id.* at 308–09.
[113] Warren & Brandeis, *supra* note 39, at 193.
[114] See Clancy, *supra* note 44, at 367–68 ("That was the essential lesson of *Katz*.").
[115] Gatewood, *supra* note 59, at 452.
[116] *See* Ferguson, *supra* note 15, at 861 (indicating that "security" is the best framework towards the protection of digital effects).

B. Reliance on Trespass is Inappropriate in a "Smart" World

The concern expressed by the Court in *Kyllo* persists: technology threatens to shrink the realm of privacy protections, now because of ambiguity in the law regarding smart objects.[117] Yet, the Fourth Amendment must protect at least the scope of rights it guaranteed at its passage: namely, security of privacy interests.[118] Justice Scalia's pivot back to trespass in *Jones* presents a problematic and overly restrictive conception of the Amendment. As it has historically, property plays a constructive role as a means of articulating what is secured by the Fourth Amendment.[119] Yet, *Jones*' literalism misconstrues the method by which the framers sought to guarantee the underlying privacy right.[120] The turn to trespass by the *Jones* Court is too dependent upon the physical to survive modern dependence on smart technologies, and it fails to properly account for the framers' methodology to guarantee the "[digital] privacies of [twenty-first century] life."[121]

In his majority opinion in *Jones*, Justice Scalia acknowledges the "close connection to property" reflected in the text of the Fourth Amendment.[122] Privacy jurisprudence, he was careful to reiterate, was tied to property at common law until *Katz*.[123] Yet, "the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."[124] Thus, Justice Scalia concluded that the corpus of Fourth Amendment law post-*Katz* remains linked to trespass, though not exclusively, as with the purely *in-rem* decisions of the Court prior to 1967.[125]

The glaring issue with Justice Scalia's recalling of trespass to the fore of privacy law is its false equivalence between exclusion and trespass.

---

[117] *See* Kyllo, 533 U.S. at 34 (noting the limitation on hits finding of unreasonableness).
[118] Jones, 565 U.S. at 406 (quoting Kyllo, 533 U.S. at 34).
[119] Carrie Leonetti, *A Grand Compromise for the Fourth Amendment*, 12 J. BUS. & TECH. L. 1, 21 (2016) ("A new doctrine of Fourth Amendment property could serve as a unifying principle to rationalize and expand the Amendment's privacy protections.").
[120] *See* Bascuas, *supra* note 43, at 622–23 (creating a property interest is "the law's vehicle for recognizing and affording privacy" as a pragmatic approach towards guaranteeing its protection).
[121] *See* Leonetti, *supra* note 119, at 21 (2016) ("High-tech invasions of privacy inflict serious harms that demand a more appropriate legal remedy than [reasonableness].").
[122] Jones, 565 U.S. at 405.
[123] *Id.* at 405–06.
[124] *Id.* at 409 (emphasis in original).
[125] *Id.* at 405–06.

For American colonialists, security in possessions was exclusive; but at that time, the distinction between exclusion and trespass—defined by a physical presence on, or in relation to, the property of another—was less clear.[126] The Supreme Court did not begin to tease out the distinction between an incursion on the effect and the information that it generated until *Katz* and its progeny;[127] indeed, the clearest analysis was not announced until 2014.[128] The physicality of trespass at the time of the Fourth Amendment's passage was not the problematic distinction it is in the modern context, since exclusion from an effect had no functional, intangible application.[129] Yet, just as the *Boyd-Olmstead-Silverman* line increasingly demonstrated that a privacy right at the mercy of trespass is vulnerable in the age of wired telecommunications, so too does the *Jones* physicality requirement enfeeble privacy in the age of IoT.

C. Exclusion Promotes an Objective Expectation of Digital Privacy

Jones' reliance on common law trespass is too restrictive to appropriately protect privacy interests in a digital age.[130] Cyberspace, of course, is not a "space" in the physical sense; it is an electronic conduit through which physical consequences may be generated.[131] Likewise, even the least intelligent, RFID-enabled smart object in the home offers "a direct portal into the data it contains, a point of 'entry' [law enforcement] can exploit without affecting any physical entry into Fourth Amendment-protected premises."[132] Under Justice Scalia's formulation, the Court "left open whether virtual intrusions" of smart objects "will also constitute a search."[133] The Court must correct its course, recognize the inapt nature of

---

[126] *See* Clancy, *supra* note 44, at 356.

[127] *See* Gatewood, *supra* note 59, at 457–58 (discussing the Court's motivation with *Katz* to address the distinction between physical and personal privacy).

[128] *See* Ferguson, *supra* note 15, at 833 (commenting on the novel analytical move in *Riley v. California*, 134 S. Ct. 2473 (2014), distinguishing "physical objects from digital content (data) in those physical objects").

[129] *See cf.* Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting) (cautioning the Court against its reliance on trespass, as "ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, [exposing] the most intimate occurrences of the home").

[130] See *infra* section III.b (arguing that smart objects in the home are effects within the meaning of the Fourth Amendment, and constitutional protection for smart effects extends to the data they generate, store, and communicate).

[131] Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1230 (2012).

[132] *Id.* at 1241–42.

[133] Ferguson, *supra* note 15, at 810; *see* United States v. Jones, 565 U.S. 400, 414, 425–26 (2012) (Sotomayor and Alito, JJ., concurring) (agreeing that *Jones*' reliance on common law trespass is too restrictive to appropriately protect digital privacy interests).

physical trespass for smart objects, and set an objective expectation of privacy based on a right to exclude.

To be sure, the *Jones* Court punted on the broader discussion of the constitutional propriety of invasive electronic surveillance, and it failed to engage in any explanation of the character of the data gathered—namely, whether it reveals enough about the "privacies of life" that collection by law enforcement of such information would, in itself, trigger the Fourth Amendment.[134] In his concurrence, Justice Alito comes closest to clarifying this more pertinent issue, which the majority opinion dismisses as beyond the scope of the matter.[135] Justice Alito rightly points out that "reliance on the law of trespass will present particularly vexing problems in cases involving surveillance . . . carried out by making electronic, as opposed to physical, contact with the item to be tracked."[136] Justice Sotomayor echoed Justice Alito's concern, noting that "physical intrusion is now unnecessary to many forms of surveillance."[137] She went further, though, to question broader societal expectations of privacy, ignored by the majority, that may be impacted by advancing technological capabilities and electronic surveillance.[138] Most conspicuously, though outside the scope of this paper, she questioned the longevity in the digital age of the Third Party Doctrine,[139] which holds individuals have no expectation of privacy regarding information disclosed to third parties, notably, to service providers.[140]

Articulating a reasonable expectation of privacy grounded in the right to exclude will bring into the sphere of the Fourth Amendment's protection smart devices that otherwise pose risks to the security of the home and the effects it contains. In line with Justices Alito and Sotomayor's concerns, the right to exclude, rather than trespass, is better suited to the non-physical technological capabilities of twenty-first century surveillance. The two concepts, both grounded in common law

---

[134] *See* Jones, 565 U.S. at 412 (acknowledging that these "vexing problems" may need to be addressed in the future "where a classic trespassory search is not involved"); *see also* Ferguson, *supra* note 15, at 810 (agreeing that the Court left open the question of whether "virtual intrusions will also constitute a search").

[135] *See* Jones, 565 U.S. at 425–26 (Alito, J., concurring) (enumerating four broad concerns left unanswered by the majority opinion).

[136] *Id.* at 426.

[137] Jones, 565 U.S. at 414 (Sotomayor, J., concurring).

[138] *See id.* at 416 (considering the "attributes of GPS monitoring" vis-à-vis societal expectations).

[139] *Id.* at 417 ("It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[140] *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

property, are related but distinct, with trespass predicated on the broader notion of exclusion.[141] Unique among property rights at common law, the right to exclude encompasses societal norms and expectations of privacy as well as offers an objective "benchmark for determining the scope of allowable intrusion into our daily lives."[142] Thus, exclusion preserves personal autonomy and protects against arbitrary intrusions by the state.[143]

Jones did not reject Justice Harlan's expectations of privacy. Per the majority opinion, where no trespassory intrusion is executed by the state, the *Katz* analysis controls.[144] What is reasonable in the context of IoT, however, is far from clear. The Court's decision in *Kyllo* gives some indication as to how a privacy right may be articulated with regards to smart objects in the home; but there, too, questions remain.[145] In contrast to *Jones*, *Kyllo* did not involve a trespass.[146] The thermal scan of the home occurred from across the street and was purely electronic.[147] In *Kyllo*, the right to exclude was tacitly supported by the Court as a corollary to the reasonable expectation of privacy.[148] Importantly though, *Kyllo* also stands for the notion that widely available technologies, or those in common use, may diminish expectations of privacy.[149] How this would play out in the context of smart objects is unclear where it is broadly understood that government agents, if not also black hat hackers, are able to remotely access smart devices in the home.[150]

Correcting its misstep in *Jones*, however, would go a long way towards correcting this uncertainty. In doing so, the Court should build on its decision in *Kyllo* and affirmatively rely on the right to exclude, while expressly recognizing the ubiquity of modern smart technology. Such a holding will have the added benefit of articulating the method by which

---

[141] See Gatewood, *supra* note 59, at 454.
[142] *Id*. at 464–65.
[143] *See* Ferguson, *supra* note 15, at 862 ("Whether conceived of as a right to be left alone, or a space for intimate activities, or other protections of personal autonomy, the Fourth Amendment has been read to encourage human development from governmental surveillance.").
[144] *See* Jones, 565 U.S. at 411
[145] *See* Gatewood, *supra* note 59, at 461.
[146] *See* Kyllo v. United States, 533 U.S. 27, 30 (2001) (noting the thermal scan was conducted from across the street, outside the curtilage).
[147] *Id*.
[148] Gatewood, *supra* note 59, at 461 (noting the reasonable expectation of privacy "preserv[ed] and protect[ed] the defendant's right to exclude even without a physical intrusion").
[149] Kyllo, 533 U.S. at 34.
[150] *See supra* notes 35–37 (detailing the known hacking capabilities of state and private actors to remotely access networked devices).

the framers intended to secure privacy.[151] Moreover, an exclusion framework, which inherently incorporates notions of reasonable expectations of privacy, would help to further assimilate digital privacy security under *Katz* by presuming exclusion as objectively reasonable.[152] This would help to focus the *Kyllo* analysis onto enhanced technologies, rather than turning on common usage—a point Justice Scalia was uncertain about in his *Kyllo* majority.[153] Thus, the pathway to a digital-privacy-protective Fourth Amendment in houses and effects would be more secure through the explicit recognition of the right to exclude.

CONCLUSION

In Fourth Amendment jurisprudence is again at a junction where relatively new, but pervasive, technologies demand a course-correction. The business model of smart devices amounts to private surveillance, and society has accepted this to the extent that it improves services through interconnectivity.[154] Yet, these devices have a range of intelligence, and each smart object represents a vector for remote access by black hat hackers and government agents alike.[155] Without an affirmative recognition by the Court that the data-rich smart home is secured by the Fourth Amendment, privacy rights in the United States are vulnerable to digital abuses by the state.

As the evolution of Fourth Amendment jurisprudence suggests, the privacy standard guaranteed by the Amendment must focus on unlawful intrusion, not the mechanism by which the intrusion is or may be perfected.[156] The method of this protection has evolved from an *in rem* focus on trespass, to the *in personam* reasonable expectation of privacy, and back to a hybrid approach defined by the physicality of the intrusion. The trespass approach re-instituted in *Jones*, however, fails to account for the potentially remote nature of government incursions at issue with the IoT and consequently, "is ill-suited to the digital age."[157] The Fourth

---

[151] *See* Clancy, *supra* note 44, at 308 (linking security to the right to exclude as the means of operationalizing privacy).

[152] *See* Leonetti, *supra* note 119, at 21 (arguing that the serious harms inflicted by high-tech invasions of privacy may best be corrected by a property-based doctrine that "serve[s] as a unifying principle to rationalize and expand the Amendment's privacy protections," like that provided by a reliance on exclusion).

[153] Kyllo, 533 U.S. at 34.

[154] *Cf.* Bruce Schneier, *The Internet of Things that Talk About You Behind Your Back*, MOTHERBOARD (Jan. 8, 2016), https://motherboard.vice.com/en_us/article/the-internet-of-things-that-talk-about-you-behind-your-back (discussing computerized devices and cyber security).

[155] Hartzog & Selinger, *supra* note 24, at 583–84.

[156] *See* Slobogin, *supra* note 97, at 162.

[157] *See* Jones, 565 U.S. at 417 (Sotomayor, J., concurring).

Amendment uses the language and concepts of property law to articulate the scope of the right protected, and it secures that right to privacy through exclusion from certain enumerated objects. The Court, therefore, must reject the overly-narrow approach of *Jones* in favor of a right to exclude that better accounts for the digital capabilities of twenty-first century surveillance. Moreover, doing so will have the added benefit of bolstering the reasonable expectation of digital privacy by presuming an objective unreasonableness in any warrantless penetration by the state into the smart home. Digital privacy is ripe for the Court's attention, and the Court should use this opportunity to "define anew . . . the extent of such protection" guaranteed by the Fourth Amendment in the age of the IoT.[158]

[158] *See* Warren & Brandeis, *supra* note 39, at 193.