California Law Review

Volume 104 | Issue 4 Article 1

8-1-2016

The Internet of Things and the Fourth Amendment of Effects

Andrew Guthrie Ferguson

Link to publisher version (DOI)
https://doi.org/10.15779/Z38JZ8G

California Law Review

VOL. 104 AUGUST 2016 NO. 4

The Internet of Things and the Fourth Amendment of Effects

Andrew Guthrie Ferguson*

ABSTRACT

"Smart objects" connected to the "Internet of Things" present new possibilities for technological surveillance. This network of smart devices also poses a new challenge for a Fourth Amendment built around "effects." The constitutional language protecting "persons, houses, papers, and effects" from unreasonable searches and seizures must confront this change. This Article addresses how a Fourth Amendment built on old-fashioned "effects" can address a new world where things are no longer just inactive, static objects, but objects that create and communicate data with other things.

DOI: http://dx.doi.org/10.15779/Z38JZ8G

* Professor of Law, David A. Clarke School of Law at the University of the District of Columbia. With thanks to Stephen Henderson and Scott Peppet for their suggestions and insights and for all of my colleagues at the Privacy Law Scholars Conference (2015) for comments and critiques.

INTRODUCTION

At the time of the American founding, "things" were tangible things. Books did not live on a cloud.[1] Horse-drawn buggies were not tracked by GPS.[2] The manor's hearth did not report the hourly change in temperature.[3] Today, with the advent of the "Internet of Things," objects in your house, car, office, and smartphone communicate, interact, report, track, and provide vast amounts of data about the activities of their owners.[4] Amazon's Kindle knows the last page you read.[5] General Motor's "OnStar System" knows the speed,

1. *See, e.g.*, Alexandra Alter, *Your E-Book Is Reading You*, WALL ST. J. (July 19, 2012), http://www.wsj.com/articles/SB10001424052702304870304577490950051438304 [http://perma.cc/GJ6M-3P85] ("The major new players in e-book publishing—Amazon, Apple and Google—can easily track how far readers are getting in books, how long they spend reading them and which search terms they use to find books."); *see also* Sean Gallagher, *Adobe's E-book Reader Sends Your Reading Logs Back to Adobe—In Plain Text*, ARS TECHNICA (Oct. 7, 2014), http://arstechnica.com/security/2014/10/adobes-e-book-reader-sends-your-reading-logs-back-to-adobe-in-plain-text [https://perma.cc/7F3V-KUJS].

2. Roger L. Easton is credited with inventing modern GPS tracking technology in the 1950s. *See* David Kravets, *GPS Inventor Urges Supreme Court to Reject Warrantless Tracking*, WIRED (Oct. 4, 2011), http://www.wired.com/2011/10/gps-inventor-surveillance [https://perma.cc/DLX3-TAVT].

3. Commercial thermostats were not invented until the 1830s, and electric room thermostats were not invented until 1883. *See* COLIN SMITH, THIS COLD HOUSE: THE SIMPLE SCIENCE OF ENERGY EFFICIENCY 164 (2012).

4. JEREMY RIFKIN, THE ZERO MARGINAL COST SOCIETY: THE INTERNET OF THINGS, THE COLLABORATIVE COMMONS, AND THE ECLIPSE OF CAPITALISM 11 (2014) ("The Internet of Things will connect every thing with everyone in an integrated global network. People, machines, natural resources, production lines, logistics networks, consumption habits, recycling flows, and virtually every other aspect of economic and social life will be linked via sensors and software to the IoT platform, continually feeding Big Data to every node—businesses, homes, vehicles—moment to moment, in real time."); *see also* DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 5–7 (2014).

5. Alter, *supra* note 1 ("Kindle users sign an agreement granting the company permission to store information from the device—including the last page you've read, plus your bookmarks, highlights, notes and annotations—in its data servers.").

direction, and travel patterns of your car.[6] The Nest Learning Thermostat knows your preferred temperature for sleeping and what time you leave home for the day.[7] "Things" have become interactive devices as a result of the growing network of ubiquitous chips and sensors placed in our everyday objects.[8]

This change poses a problem for a Fourth Amendment protecting "persons, houses, papers, and *effects*" from unreasonable searches and seizures.[9] This Article explores how a Fourth Amendment built on old-fashioned "effects" can address a new world in which things are no longer just inactive, static objects, but objects that create and communicate data with other things.

The Article seeks to answer two questions. First, how is a Fourth Amendment "effect" defined in a world animated by an interconnected, network-like Internet of Things (IoT)? Second, what expectation of security should attach to these IoT effects?[10] These questions are critical: unless our constitutional understanding of an effect adapts to meet modern technology, smart objects will be open to warrantless searches without sufficient Fourth Amendment protection.

As to the first definitional question, this Article argues that Fourth Amendment effects can include smart objects *and related data* that populate the Internet of Things.[11] As a doctrinal matter, the Fourth Amendment has evolved beyond narrow constitutional definitions.[12] "Persons" include more than just physical bodies; they now include clothing, bodily fluids, DNA, and

6. Kevin Rector, *Debate Over Web-Connected Cars, Driver Privacy Headed to Maryland*, BALT. SUN (Aug. 2, 2014, 4:44 PM), http://www.baltimoresun.com/business/bs-bz-connected-cars-20140802-story.html [https://perma.cc/VTY8-2PVT] ("OnStar acknowledged that it collects a wide variety of information about its users and their vehicles, including their location and speed. It said it keeps the data as long as it wants . . . ."); *see also* Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 705 (2014) ("Ford Motor Company's top sales executive recently made headlines when he bragged, 'We know everyone who breaks the law. We know when you're doing it. We have GPS in your car, so we know what you're doing.'").

7. Caleb Garling, *Google Enters Homes with Purchase of Nest*, S.F. CHRON., Jan. 14, 2014, at D6 ("Palo Alto's Nest is a flagship brand in the burgeoning Internet of Things—a catchphrase for a wave of tech innovations that could turn once-mundane appliances like ovens, thermostats, microwaves, fridges and garage-door openers into a network of devices that communicate with each other."); *see* NEST, https://nest.com [https://perma.cc/5MGD-KUBB] (last visited Mar. 28, 2016).

8. *See infra* Part I.

9. U.S. CONST. amend. IV (emphasis added).

10. Use of the term "security" is purposeful, as security offers a different level of protection than "privacy." *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 349–50 (1998); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008) ("The Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of security.").

11. *See infra* Part III.

12. *See infra* Part III.A.

even corporations.[13] "Houses" now include curtilage, barns, apartments, and commercial spaces.[14] "Papers" now include digital recordings, writings, business documents, and other communications.[15] So too with "effects": courts can create an updated understanding relevant to the digital world, but consistent with Fourth Amendment principles.[16] This definition would include a defined portion of the effect's functionality including its necessary communication with other devices and stored data.[17] An "effect" would not only be the physical object but also the smart data and communicating signals emanating from the device.

As to the second question regarding security, once effects are defined as not just physical objects, but also those objects' accompanying data and communications signals, the threshold question whether officials have conducted a Fourth Amendment search becomes quite complicated.[18] Is the virtual recovery of stored data in a device a search? Is the interception of wireless data from interconnected sensors a search?[19] Demarcating a threshold of privacy-security in a nonphysical world presents real challenges to technology and Fourth Amendment doctrine.[20] This Article seeks to redefine an effect and answer these difficult line-drawing questions.

This Article proposes a theory of "digital curtilage" as a framework to address the definitional and security questions presented by the Internet of Things. Inspired by the concept of physical curtilage traditionally used to protect the space and activities surrounding the home,[21] but not actually part of the home, digital curtilage provides limited Fourth Amendment protection for personal data from networked devices. Digital curtilage protects stored data and certain communication signals that: (1) are closely associated with the effect; (2) have been marked out and claimed as secure from others; and (3) are used to promote personal autonomy, family, self-expression, and association.[22]

The need for a new theory arises out of two changes: one of law and the other of technology. First, as a matter of Fourth Amendment law, the Supreme

13. *See infra* Part III.A.1.
14. *See infra* Part III.A.2.
15. *See infra* Part III.A.3.
16. *See infra* Part III.A.4.
17. *See infra* Part III.C.
18. While complicated, the answer to this question is critical because without a threshold determination of an effect, there can be no Fourth Amendment search under a physical trespass-physical invasion theory.
19. From another analytical approach one could consider this action a Fourth Amendment seizure. This Article does not address the issue of seizure. *See* Paul Ohm, *The Olmstedian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2.
20. Debra Cassens Weiss, *Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question*, ABA J. (Mar. 24, 2014), http://www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a [http://perma.cc/BMY5-2PPK].
21. *See* Oliver v. United States, 466 U.S. 170, 177 (1984).
22. *See infra* Part IV (describing the theory of digital curtilage in detail).

Court's recent decisions in *United States v. Jones*[23] and *Florida v. Jardines*[24] have rejuvenated the concept of "constitutionally protected interests" such as effects.[25] This traditional conception of Fourth Amendment law must once again be considered to determine whether a trespass or other physical intrusion has occurred. *Jones*, itself, involved a trespass on an effect (a car).[26] The Court left open whether virtual intrusions will also constitute a search, but scholars including myself have argued for consideration of a broader understanding covering such sense-enhanced intrusions.[27] The reemergence of traditional terms of art such as "effects" adds new urgency to a redefinition of the terms consistent with modern technology (and even modern physics).[28] In addition, the Supreme Court's 2014 decision in *Riley v. California*,[29] concerning the warrantless search of smartphone data incident to arrest, highlights a new distinction between ordinary effects and digital information produced by an effect.[30]

The second change is that the Internet of Things has emerged as a new technological puzzle filled with risks involving security, privacy, and personal liberty.[31] The Internet of Things offers new surveillance possibilities that do not involve any physical intrusion into the object. As currently designed, these objects radiate data trails quite useful for law enforcement tracking.[32] Further,

---

23. 132 S. Ct. 945 (2012).

24. 133 S. Ct. 1409 (2013).

25. *See generally* Jack Wade Nowlin, *The Warren Court's House Built on Sand: From Security in Persons, Houses, Papers, and Effects to Mere Reasonableness in Fourth Amendment Doctrine*, 81 MISS. L.J. 1017, 1031–32 (2012) (discussing the protected interests approach as the "traditional approach emphasized the interests specifically enumerated as protected in the text of the Fourth Amendment, 'persons, houses, papers, and effects,' and the common-law principles rooted in property law that formed the important broader legal context of the text").

26. *Jones*, 132 S. Ct. at 948.

27. *See* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1328–40 (2014); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 438 (2002).

28. *See, e.g.*, Jim Harper, *Escaping the Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2011–12 CATO SUP. CT. REV. 219, 232 (2008); Steven Kam, Intel Corp. v. Hamidi*: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427, 440 (2004) ("A modern understanding of physics blurs the line between actions that qualified traditional trespass, such as bodily intrusion and bricks thrown through windows and 'intangible' invasions now understood to be 'physical,' such as particulate matter (smog, industrial fumes) and electromagnetic energy.").

29. 134 S. Ct. 2473 (2014).

30. *Id.* at 2489 (recognizing the difference in quality and quantity of digital information stored in a smartphone).

31. *See infra* Part I.

32. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 120 (2014) ("The technical problem created by the Internet of Things is that sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources. Put simply, in a world of connected sensors, 'everything may reveal everything.' Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of—and perhaps all—other economic or information contexts."); Neil M. Richards, *The Dangers of Surveillance*, 126

the commonality of these communicating devices will alter our relationship with the technology. Studies report that by 2020, there will be over fifty billion interconnected devices linking the world together.[33] Those devices will create a web of information that—coupled with big data surveillance techniques—could produce a real threat to Fourth Amendment liberties. Many sensor devices will no longer be opt-in technologies but will be built within our homes, cars, offices, and play spaces.[34] More relevant to this Article, what we ordinarily think of as static objects will become communication tools, revealing our paths, interests, habits, and lives to companies and law enforcers.[35] As police investigators discover the utility of tracking capabilities in these objects, new Fourth Amendment questions will emerge.

How the Fourth Amendment adapts to these new surveillance systems will be a central issue in the coming years. This Article seeks to establish a framework for analyzing the Internet of Things within the current Fourth Amendment doctrine, as well as to show the existing gaps in coverage. The Article then seeks to provide an alternative theoretical framework based on digital curtilage to fill these doctrinal gaps.

Part I of this Article examines the rise of the Internet of Things[36] and the advanced surveillance capabilities offered by these devices. Part II examines the concept of Fourth Amendment "effects" from the founding to the present day and reveals the shortcomings of current doctrine as applied to smart effects located in homes, on persons, and in cars. Part III argues that the term "effects," like other Fourth Amendment terms,[37] should evolve to embrace a definition broader than merely the physical object involved. Part IV introduces the theory of digital curtilage. Building off of the concept of physical curtilage, this Article posits the theory of digital curtilage as a framework to analyze

---

HARV. L. REV. 1934, 1936, 1940 (2013) (recognizing that the Internet of Things will permit "previously unobservable activity to electronic measurement, observation, and control").

33. Tony Danova, *Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020*, BUS. INSIDER, (Oct. 2, 2013, 4:16 PM), http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10 [http://perma.cc/VH4G-A4GE] ("Cisco thinks about 50 billion devices will be connected by 2020, after coming out with an earlier analysis in January that claimed 8.7 billion connected devices in 2012. A separate analysis from Morgan Stanley feels that number can actually be as high as 75 billion . . . .").

34. Mohana Ravindranath, *Building the 'Internet of Things,'* WASH. POST (Aug. 30, 2013), http://www.washingtonpost.com/business/on-small-business/building-the-internet-of-things/2013/08/29/e3fbc1ae-1024-11e3-85b6-d27422650fd5_story.html [http://perma.cc/CR2U-ZKM2].

35. *See, e.g.*, Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, *Promoting an Internet of Inclusion: More Things and More People* (Jan. 8, 2014), 2014 WL 585463, at *2 ("Mobile devices also play an important role in the Internet of Things as they collect, analyze, and share information about users and their environments, such as their current location, travel patterns, speeds, and the noise levels in their surroundings.").

36. Peppet, *supra* note 32, at 89 n.13 (citing Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/pdf?4986 [http://perma.cc/B4CW-M29Z]).

37. *See infra* Part III.

smart "effects" in the Internet of Things. Although the task of redefining a foundational term of art in the Fourth Amendment may meet some justifiable skepticism, "digital curtilage" fills the existing doctrinal gaps and offers a way forward consistent with both law and technology.

I.
THE INTERNET OF THINGS

As a general matter, the concept behind the Internet of Things is quite simple: objects embedded with identifiers or recognizable by sensors will be able to communicate digital information to sensors seeking to collect the information.[38] Networks of "intelligent"[39] or "enchanted"[40] objects will be developed to improve consumer, commercial, health, and other needs. Whether it is a pill bottle that reminds you to take your medicine,[41] a refrigerator that automatically orders milk when you run out,[42] or tires that alert you before they become deflated,[43] objects will collect and share data in an effort to be more efficient or user-friendly to their owners. This data can be locally stored, wirelessly shared, or centrally collected through Internet applications to allow monitoring of the relevant information.[44]

---

38. Luigi Atzori et al., *The Internet of Things: A Survey*, 54 COMPUTER NETWORKS 2787, 2787 (2010) ("The basic idea of this concept is the pervasive presence around us of a variety of things or objects—such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc.—which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals."); *see id.* at 2789 (explaining the European Commission's current definition: "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"); Peppet, *supra* note 32, at 98 ("Microelectromechanical systems (MEMS) sensors translate physical phenomenon, such as movement, heat, pressure, or location, into digital information.").

39. Paul Kominers, *Interoperability Case Study, Internet of Things (IoT)*, BERKMAN CTR. FOR INTERNET & SOC'Y (Apr. 16 2012), https://cyber.law.harvard.edu/node/97248 [https://perma.cc/VG3W-4DER] ("The grand vision of the Internet of Things (IoT) is a world of networked intelligent objects. Every car, refrigerator, and carton of milk would be distinguished with its RFID chip, and they communicate constantly and seamlessly to create a much more efficient world.").

40. Rose, *supra* note 4, at 7 (defining an enchanted object as "ordinary things made extraordinary").

41. *Id.* at 9 (detailing a "magic" pill bottle called "GlowCap" that glows and communicates via the Internet).

42. Kominers, *supra* note 39; RICHARD L. RUTLEDGE ET AL., GA. INST. OF TECH., DEFINING THE INTERNET OF DEVICES: PRIVACY AND SECURITY IMPLICATIONS (2014), https://smartech.gatech.edu/bitstream/handle/1853/52020/plsc2014-IoD.pdf [https://perma.cc/3C4K-A92H].

43. Sinem Coleri Ergen et al., *The Tire as an Intelligent Sensor*, 28 IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS & SYSTEMS 941, 942–43 (2009), http://www.isr.umd.edu/~austin/enes489p/project-resources/EE249-Tire-Sensor.pdf [https://perma.cc/6DSW-LGGL].

44. Quentin Hardy, *Cloud Technology, in Translation*, N.Y. TIMES, June 12, 2014, at F2 ("Internet of Things: The idea of an Internet on which millions of industrial and personal objects are connected, usually through cloud systems. The objects would deliver sensor information, and possibly modify themselves, to create overall management of a larger system, like a factory or city.").

Experts predict that the worldwide scale of such "smart," interconnected objects will continue to grow, reaching more than fifty billion objects in 2020,[45] and one trillion by 2025.[46] As inexpensive, unobtrusive identifying technology combines with more sophisticated wireless networks, new possibilities will emerge to allow tracking of human and nonhuman activity.[47] The result will be additional options for government surveillance that can reveal the patterns of everyday life.[48]

This Part provides a general overview of the existing technologies. After a brief history of the development of the Internet of Things, this Part also examines some of the potential uses for law enforcement and then some of the definitional challenges arising from the technologies.

A. A Brief History of the Internet of Things

Technologist Kevin Ashton coined the term "the Internet of Things" in 1998 during a presentation to Procter and Gamble when he stated, "Adding radio-frequency identification and sensors to everyday objects will create an Internet of Things, and lay the foundations of a new age of machine perception."[49] The visionary concept was that radio-frequency identification devices (RFID) chips could be used to order, track, and study manufacturing processes in a new manner. RFID chips provide unique identifiers embedded in objects that can be tracked and monitored.[50] While this idea of a networked

45. RUTLEDGE ET AL., *supra* note 42; Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 218 (2012) ("Cisco estimates that by 2020 there will be 50 billion connected devices, 7 times the world's population.").

46. Peppet, *supra* note 32, at 98 & n.54 (citing Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013), http://www.wired.com/2013/05/internet-of-things-2/all [http://perma.cc/8EM3-VKP9]).

47. Swan, *supra* note 45, at 218 ("'The Internet of Things' is the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and controllable via the Internet—whether via RFID, wireless LAN, wide-area network, or other means.").

48. Steve Lohr, *The Age of Big Data*, N.Y. TIMES (Feb. 11, 2012), http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html [https://perma.cc/J8Y3-QEWX] ("[T]here are now countless digital sensors worldwide in industrial equipment, automobiles, electrical meters and shipping crates. They can measure and communicate location, movement, vibration, temperature, humidity, even chemical changes in the air. Link these communicating sensors to computing intelligence and you see the rise of what is called the Internet of Things or the Industrial Internet.").

49. Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 [https://perma.cc/X679-AWNF]; RUTLEDGE ET AL., *supra* note 42.

50. Alexandre Santos et al., *Internet of Things and Smart Objects for M-Health Monitoring and Control*, 16 PROCEDIA TECH. 1351, 1352 (2014) ("The Radio-Frequency IDentification, commonly known as RFID, is used in many applications. . . . There are several methods of identification, although the most common is a microchip able to store a serial number that identifies the person, object or thing. Using electronic devices that emit radio frequency signals, it is possible to perform an automatic capture of data, or a tag, from a reader."); *see id.* at 1353 ("[RFID] tags may be

manufacturing process dates back to the late 1980s,[51] and the future vision extends well beyond commercial infrastructure to "the Internet of Everything,"[52] the early developments centered on commercial innovation.

In fact, the use of RFID tags[53] and sensors helped spark a revolution of industrial design and processing. Engineers developed smart factories that relied on sensor technology to organize, monitor, and track manufacturing processes and worker productivity.[54] Manufacturing companies realized that parts could be tracked along the production line, speeding up delivery times, regulating inventory, and improving outputs.[55] A company could track a widget from production in China, to assembly in Indonesia, to sale in America.[56] Consumer companies realized they could track every item sold (sweaters, cars, computers, etc.) through RFID chips and sensors,[57] manage inventories with real-time precision,[58] and target retail sales at the micro level.[59] Further, for more sophisticated items, sensors could warn of needed repairs and

classified as Read Only (RO), Write Once Read Many (WORM) and Write Many Read Many (WMRM) corresponding the type of the access to information that is kept in its memory structure.").

51. *A Sea of Sensors*, ECONOMIST (Nov. 4, 2010), http://www.economist.com/node/17388356 [https://perma.cc/845L-D7N4] ("The concept of the 'internet of things' dates back to the late 1980s, when researchers at Palo Alto Research Centre (PARC) in Silicon Valley imagined a future in which the virtual and the real world would be connected.").

52. DAVE EVANS, CISCO, THE INTERNET OF EVERYTHING: HOW MORE RELEVANT AND VALUABLE CONNECTIONS WILL CHANGE THE WORLD 1 (2012), https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf [https://perma.cc/6Y6H-L29A].

53. Atzori et al., *supra* note 38, at 2790 ("[RFID] tags are characterized by a unique identifier and are applied to objects (even persons or animals). Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs. Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the *real world* into the *virtual world*.").

54. *See, e.g.*, Christopher Alessi & Chase Gummer, *Germany Bets on 'Smart Factories' to Keep Its Manufacturing Edge*, WALL ST. J. (Oct. 26, 2014), http://www.wsj.com/articles/germany-bets-on-smart-factories-to-keep-its-manufacturing-edge-1414355745 [http://perma.cc/PW6B-Q5J9].

55. Chloe Green, *The Internet of Things Business Process Revolution*, INFO. AGE (Sept. 10, 2014), http://www.information-age.com/it-management/strategy-and-innovation/123458453/internet-things-business-process-revolution [http://perma.cc/3DVQ-444L].

56. *See, e.g.*, Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695, 696 (2006) (discussing inventory control and manufacturing applications of RFID technology).

57. Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 135 (2006); Wang Zhengxia & Xiao Laisheng, *Modern Logistics Monitoring Platform Based on the Internet of Things*, 2010 INT'L CONF. ON INTELLIGENT COMPUTATION TECH. & AUTOMATION 726, 727–29, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5522698 [http://perma.cc/E8MP-QTBR].

58. Julie Manning Magid et al., *Radio Frequency Identification and Privacy Law: An Integrative Approach*, 46 AM. BUS. L.J. 1, 4 (2009) ("With the advent of RFID, Marks & Spencer adopted realtime inventory control. It began putting RFID tags at the item level, a trial that expanded to all its stores.").

59. Faheem Zafar et al., *Micro-location for Internet of Things Equipped Smart Buildings*, 3 IEEE INTERNET OF THINGS J. 96 (2016) (describing applications such as a customer being greeted at the door of a store or receiving advertisement through micro targeting).

performance outcomes.[60] This resulted in a series of local networks that allowed for sophisticated data collection.

Building off these RFID innovations, engineers developed wireless sensor networks to observe objects and relay that observation back to a central location in a factory.[61] Machines were programed to sense the position of physical objects on the factory floor. Just as RFID tags enabled manufacturing companies to smooth their supply chain, wireless sensor networks helped improve the factory automation process.[62]

In addition to businesses, government officials designed wireless sensors to monitor users of public services.[63] Thus, cars could be studied to gauge traffic flow, patients could be tracked through their time at a hospital, and museum visitors could be monitored (and guided) through attractions and exhibits.[64] Smart electricity grids now monitor real-time usage across large geographic areas.[65] Automatic sensors monitor license plates,[66]

60. Steve Lohr, *The Internet Gets Physical*, N.Y. TIMES (Dec. 11, 2011), http://www.nytimes.com/2011/12/18/sunday-review/the-internet-gets-physical.html [http://perma.cc/86E7-Y7RK] ("Across many industries, products and practices are being transformed by communicating sensors and computing intelligence. The smart industrial gear includes jet engines, bridges and oil rigs that alert their human minders when they need repairs, before equipment failures occur. Computers track sensor data on operating performance of a jet engine, or slight structural changes in an oil rig, looking for telltale patterns that signal coming trouble.").

61. Atzori et al., *supra* note 38, at 2790; Geng Wu et al., *M2M: From Mobile to Embedded Internet*, IEEE COMM. MAG. (Apr. 2011), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5741144 [https://perma.cc/97T6-NWCV] (discussing machine-to-machine technologies and the embedded Internet).

62. RUTLEDGE ET AL., *supra* note 42.

63. B.A. Li, *Smart Transportation Service Based on Social Computing and SOA*, *in* REMOTE SENSING AND SMART CITY 54, 54–56 (Chou T. ed., 2015) (discussing how public transportation can be improved by the Internet of Things); Patrick Thibodeau, *Explained: The ABCs of the Internet of Things*, COMPUTERWORLD (May 6, 2014, 7:30 AM), http://www.computerworld.com/article/2488872/emerging-technology-explained-the-abcs-of-the-internet-of-things.html [http://perma.cc/WUF8-UCUP].

64. Wu et al., *supra* note 61 (discussing the uses of the Internet of Things in the physical world); *Evidence From Black Boxes in Cars Turns Up in Courts*, FOX NEWS (June 28, 2003), http://www.foxnews.com/story/0,2933,90673,00.html [http://perma.cc/DN3U-UK4A]; Bob Gritzinger, *Under the Hood, with Big Brother: Forget Orwell's 1984—20 Years Later It's Our Cars That Are Giving Us Up*, AUTOWEEK (Nov. 7 2004), http://autoweek.com/article/car-news/under-hood-big-brother-forget-orwells-198420-years-later-its-our-cars-are-giving-us [http://perma.cc/T9BA-MV56]; Steve Lohr, *Looking to Industry for the Next Digital Disruption*, N.Y. TIMES, Nov. 11, 2012, at B1 ("For the last few years, G.E. and Mount Sinai Medical Center have been working on a project to optimize the operations of the 1,100-bed hospital in New York. Hospitals, in a sense, are factories of health care. . . . At Mount Sinai, patients get a black plastic wristband with a location sensor and other information. Similar sensors are on beds and medical equipment. An important advantage, . . . is to be able to see the daily flow of patients, physical assets and treatment as it unfolds.").

65. Jan Beyea, *The Smart Electricity Grid and Scientific Research*, 328 SCIENCE 979 (2010); Andreas Kamilaris et al., *Integrating Web-Enabled Energy-Aware Smart Homes to the Smart Grid*, 5 INT'L J. ON ADVANCES INTELLIGENT SYSTEMS 15 (2012), http://www.iariajournals.org/intelligent_systems [http://perma.cc/XS5Z-5A8A].

66. Stephen Rushin, *The Judicial Response to Mass Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 286 (2011) ("ALPR [Automatic License Plate Recognition] systems not only flag passing cars that match a criminal database, but they also record the exact time and location of *all passing cars*

human faces,[67] and even environmental toxins.[68] The result is that patterns of human activity are tracked and mapped, revealing numerous personal details otherwise not observable to the public.

As companies began to see that ordinary items could provide valuable information about consumer habits and preferences, they quickly adapted these industrial and governmental innovations to the consumer space.[69] Just as big data companies had been mining the Internet and social media for personalized information about consumers,[70] IoT companies recognized that the items themselves could reveal patterns useful for future marketing. While Amazon might know you purchased new running shoes, Fitbit knows whether you used them.[71] And, the level of detail can be humorously specific. As one commentator wrote:

> In a world where objects are connected to the Internet, you could imagine one sock emailing the other to say it fell behind the dryer,

---

into a searchable database, whether or not there is any evidence of wrongdoing. This data can be kept on file indefinitely. In communities with extensive, integrated networks of ALPR cameras, this could potentially amount to mass surveillance of an entire community.") (emphasis added); Martin Kaste, *Police May Know Exactly Where You Were Last Tuesday*, NPR (July 17, 2013), http://www.npr.org/sections/alltechconsidered/2013/07/16/202801282/police-may-know-exactly-where-you-were-last-tuesday [https://perma.cc/4XLE-72ZB].

67. David Goldman, *Real-Time Face Recognition Comes to Your iPhone Camera*, CNN MONEY (Mar. 12, 2012, 11:13 AM), http://money.cnn.com/2012/03/12/technology/iPhone-face-recognition [http://perma.cc/8FSD-QR9Q]; *see also* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 447–48 (2012); Sabrina A. Lochner, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 206 (2013); Rushin, *supra* note 66, at 288.

68. Swan, *supra* note 45, at 227 ("More generally, it is now possible to use environmental sensors to measure a range of concerns including air quality, barometric pressure, carbon monoxide, capacitance, color, gas leaks, humidity, hydrogen sulfide, temperature, and light.").

69. *See id.* ("[E]veryday objects that have not previously seemed electronic at all are starting to be online with embedded sensors and microprocessors, communicating with each other and the Internet. This includes items such as food, clothing, household appliances, materials, parts, subassemblies, commodities, luxury items, landmarks, buildings, and roads."); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015).

70. JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 3 (2014); Elspeth A. Brotherton, Comment, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 563 (2012); Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950, 991 (describing how companies can "provide lists of people who take Prozac for depression, believe in the Bible, gamble online, or buy sex toys").

71. Even simple data about walking can be quite revealing. Robert Vamosi, *IoT (and Big Data) Underfoot*, FORBES (Dec. 29, 2014, 1:30 PM), http://www.forbes.com/sites/robertvamosi/2014/12/29/iot-and-big-data-underfoot [http://perma.cc/4X4L-YH4C] (discussing how even your footsteps (or gait) tracked by fitness bands can reveal health habits: "There's enormous interest within the IoT community about how precisely your foot lands each time you take a step. Footfall, more accurately your gait, says a lot about your current state of health, whether it is the onset of multiple sclerosis or some other neurological disease. Even whether or not you took your daily cocktail of meds, or whether they are still as effective today as when they were first prescribed").

> your car would know when your carburetor is acting up and automatically set up an appointment with your mechanic to fix the issue, or the buttons on your shirt could be heart monitors that notify your doctor if you're not feeling well.[72]

Mapping consumer interests at an extremely personal level has become a growing and quite lucrative business, with many big technology companies jumping into the field.[73]

While still in the infancy of the consumer age of the Internet of Things, the number of companies providing IoT-related services and goods continues to grow.[74] Wearable sensors that monitor health and fitness can now be found in clothes, in wristbands, and even implanted in human bodies or placed on medical bandages or removable tattoos.[75] In addition, sensors in homes can adjust heating, lighting, and open the garage door when we return home from work.[76] Sensors in cars can reveal automotive performance and a driver's location, speed, and actions in real time.[77] Currently, the website

---

72. Nick Bilton, *Some Predictions About the Internet of Things and Wearable Tech from Pew Research*, N.Y. TIMES: BITS (May 14, 2014, 10:00 AM), http://bits.blogs.nytimes.com/2014/05/14/some-predictions-about-the-next-decade-from-pew-research [http://perma.cc/VL33-VVG2].

73. JAMES MANYIKA ET AL., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 51 (2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies [http://perma.cc/KG6X-CLVZ] (projecting $2.7 trillion to $6.2 trillion per year by 2025); Gil Press, *Internet of Things by the Numbers: Market Estimates and Forecasts*, FORBES (Aug. 22, 2014, 1:17 PM), http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts [http://perma.cc/ZTQ6-2PHZ].

74. Timothy B. Lee, *Everything's Connected: How Tiny Computers Could Change the Way We Live*, VOX (Aug. 13, 2014), http://www.vox.com/2014/5/8/5590228/how-tiny-computers-could-change-the-way-we-live [http://perma.cc/69PE-MBRD]; Bill Wasik, *Why Wearable Tech Will Be as Big as the Smartphone*, WIRED (Dec. 17, 2013, 6:30 AM), http://www.wired.com/gadgetlab/2013/12/wearable-computers [http://perma.cc/NE7Y-PXTQ].

75. Swan, *supra* note 45, at 218. It is estimated that 80 million wearable sensors will be in use for health-related applications by 2017, an eight-fold increase over today. These stretchable electronics track and wirelessly transmit information such as heart rate, brain activity, body temperature, and hydration level, and may be available to athletes in the fall of 2012. *Id.* at 222; *see also* Keiron Monks, *Forget Wearable Tech: Embeddable Implants Are Already Here*, CNN (Apr. 8, 2014, 1:08 PM), http://www.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants [http://perma.cc/63EK-P8US]; Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014, 1:26 PM), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance [http://perma.cc/D3S5-4GC2]; HEXOSKIN, http://www.hexoskin.com (last visited Mar. 28, 2016).

76. Atzori et al., *supra* note 38, at 2795 ("Sensors and actuators distributed in houses and offices can make our life more comfortable in several aspects: rooms heating can be adapted to our preferences and to the weather; the room lighting can change according to the time of the day; domestic incidents can be avoided with appropriate monitoring and alarm systems; and energy can be saved by automatically switching off the electrical equipments when not needed.").

77. Swan, *supra* note 45, at 218 ("It is estimated that 90% of new vehicles sold in 2020 will have on-board connectivity platforms, as compared with 10% in 2012.").

"quantifiedself.com"[78] lists hundreds of tools to monitor exercise, moods, sleep patterns, and food intake among other quantifiable actions we take in life.[79]

Wireless networks have necessarily grown to keep pace with the use of personal wireless devices such as smartphones, computers, and tablets.[80] While not always recognized by consumers as being part of the Internet of Things, these networks have the potential to identify users through the "things" they carry with them from place to place.[81] Many cellphones have unique identifiers and each computer or tablet has an identifiable Internet Protocol (IP) address linked to a service provider or Ethernet address, all of which provide a simple mechanism to track individuals using cellular, Wi-Fi, and other data networks.[82]

While one must be cautious about overhyping the "next big thing" in technology, the momentum toward a connected world of communicating objects is close at hand. The rapid growth of personal consumer devices heralds a new world of personal effects, many of which have the potential to become little spies on their users. These enchanted personal effects, not the industrial or commercial applications of the technology, are the subject of this Article.

B. The Internet of Things and Advanced Surveillance Capabilities

The Internet of Things is by design a system of surveillance.[83] Current technology based on sensor and Wi-Fi communications offers minimal security

78. *Guide to Self Tracking Tools*, QUANTIFIED SELF, http://quantifiedself.com/guide (last visited Mar. 29, 2016).

79. There is a widespread trend and market for monitoring life habits. *See, e.g.*, Thierer, *supra* note 69; Alex Jinsung Choi, *Internet of Things: Evolution towards a Hyper-Connected Society*, IEEE ASIAN SOLID-STATE CIRCUITS CONFERENCE 5 (2014), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7008846 [http://perma.cc/BYL6-9B9J] (discussing consumer growth); *The Quantified Self: Counting Every Moment*, ECONOMIST (Mar. 3, 2012), http://www.economist.com/node/21548493 [http://perma.cc/BYL6-9B9J].

80. *See, e.g.*, Daniel A. Reed et al., *Imagining the Future: Thoughts on Computing*, 45 COMPUTER 25, 25–30 (2012); Erin Mershon, *Apple Dives into 'Internet of Things,'* POLITICO (June 2, 2014, 6:01 PM), http://www.politico.com/story/2014/06/apple-wwdc-2014-internet-of-things-107336.html#ixzz33hMxZTIN [http://perma.cc/34SM-VGC8].

81. *See, e.g.*, JAMES MANYIKA ET AL., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 85 (2011) ("As the number of people using mobile phones has increased, the use of cell-tower signals to triangulate the location of such devices has become increasingly common. This technology has the potential to identify the location of the owners of almost 5 billion globally.").

82. Ohm, *supra* note 19, at 43 ("In most cities, ubiquitous WiFi networks allow users to transmit data over the Internet using radio waves. With specialized but inexpensive equipment, WiFi signals can be intercepted. Although WiFi can be encrypted, some forms of WiFi encryption are notoriously insecure."); Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1081 (2013) (discussing phones); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1837 (2011) (discussing computers).

83. Nancy J. King, *When Mobile Phones Are RFID-Equipped—Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L.

protection (at least from sophisticated parties).[84] Sensors vary from the highly secure to the simplistic, with equally varying levels of encryption and protection.[85] The current framework, thus, provides new surveillance opportunities for law enforcement—with or without the proper legal authority[86]—to monitor citizens suspected of crime.[87] Just as businesses can use the highly personal data to target consumers, so too can police use such data to target suspected criminals.[88] Just as surveillance technology has evolved in many other areas, the Internet of Things provides enhanced new surveillance structure worth exploring. This Section addresses the technological possibilities of the Internet of Things. Specifically, this Section examines the consequences of a seamless, secret, and occasionally sentient technology that offers new surveillance possibilities.

By being seamless, IoT technology has the potential to generate an almost inescapable data web that monitors many aspects of one's life.[89] From home

---

REV. 107, 143–44 (2008) ("If the information stored on an RFID-tagged consumer item is unique to the particular item, it can be used to distinguish the person carrying the item from all other persons and thus be used to track the person carrying the RFID-tagged item.").

84. *See A Brief History of Wi-Fi*, ECONOMIST (June 10, 2004), http://www.economist.com/node/2724397 [http://perma.cc/T2RU-BTPP]; Paul Wagenseil, *Google Spy Case Shows Why You Need to Encrypt Your Wi-Fi*, NBCNEWS.COM (May 1, 2012, 9:19 AM), http://www.nbcnews.com/id/47237136/ns/technology_and_science-security/t/google-spy-case-shows-why-you-should-encrypt-your-wi-fi [http://perma.cc/FNB3-65NJ] ("Hackers snooping on unprotected or poorly protected Wi-Fi networks have been responsible for some of the biggest cyberheists in recent history, including numerous thefts from Seattle-area businesses from 2006 to 2011 and the 2007 TJX Companies data breach, which exposed 45 million credit-card numbers.").

85. Some recent studies suggest that one-third of Wi-Fi networks remain unsecured. *See* Carla Voigt, Note, *Wi-Fi Security: Shaping Data Privacy Rules*, 66 FED. COMM. L.J. 537, 541 (2014). Because many of the sensors in the Internet of Things are even less sophisticated than Wi-Fi networks, the dangers of unprotected data remain a real issue. *See also* Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES, Feb. 16, 2011, at B8 ("Until recently, only determined and knowledgeable hackers . . . could spy while you used your laptop or smartphone at Wi-Fi hot spots. But a free program called Firesheep . . . has made it simple to see what other users of an unsecured Wi-Fi network are doing and then [impersonate] them [on] sites they visited.").

86. This Article focuses on the constitutional limitations to law enforcement. Statutory authority may provide a measure of protection from law enforcement surveillance. Currently, a draft of the new Electronic Privacy and Computer Act includes additional protection against wireless surveillance. *But see* Matthew Mason, Comment, *Aligning Online Privacy Protection with Reasonable Expectations of Privacy: How* Joffe *Can Be Used to Modernize the Wiretap Act*, 15 MINN. J.L. SCI. & TECH. 1155, 1160 (2014) (discussing legislative proposals to modernize the Wiretap Act to explicitly cover wireless interception of data).

87. *See, e.g.*, Ohm, *supra* note 19, at 44 ("Like WiFi, Bluetooth security has been criticized and attacked, and there have been reports of so-called Bluetooth sniffing, techniques which the police could use to download a target's address book or calendar from half-a-block away.") (citing Annalee Newitz, *They've Got Your Number* . . ., WIRED (Dec. 1, 2004), http://www.wired.com/2004/12/phreakers [https://perma.cc/4UP8-CKDA] (describing Bluetooth attacks on cellphones)).

88. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 329 (2015).

89. *See* Nicolas P. Terry, *Protecting Patient Privacy in the Era of Big Data*, 81 UMKC L. REV. 385, 389–90 (2012) ("Increasingly and of considerable importance going forward, big data comes from less structured sources including 'web-browsing data trails, social network communications, sensor data and surveillance data.' Much of it is 'exhaust data,' or data created

appliances, to cars, to medical devices, the array of objects is continuously digitizing daily activities.[90] While society has recently been made aware of possible high-tech surveillance techniques involving cameras, drones, GPS tracking, and cellphone collection,[91] it has not always envisioned the linkage of disparate technologies on a very personal level. Knowing you called a certain number (cell data), drove to a certain house (drone or camera), and repeated that trip every week (GPS) pales in comparison to knowing those facts *plus* the time the bedroom light comes on in that house (through NEST systems), the elevated heartbeat in that bedroom (through health monitors), and the opening of a particular enchanted pill bottle (smart pill bottles)—all of which might provide a much better clue about the nature of your business at the house.[92] Problems of aggregation[93] and magnification[94] heighten the potential personal invasion as a data-rich environment creates a wider mosaic of life patterns.[95] Police might no longer need to physically follow a suspect—smart sensors allow them to do so virtually. [96]

Most police surveillance is, by definition, secret (at least for the person being spied upon). The Internet of Things involves the potential secret interception of data through both direct and indirect means.[97] Devices that directly capture wireless communication from IoT-connected devices enable

---

unintentionally as a byproduct of social networks, web searches, smartphones, and other online behaviors.").

90. *See* John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES (Nov. 29, 2008), http://www.nytimes.com/2008/11/30/business/30privacy.html [http://perma.cc/XW77-YKZM].

91. *See generally* Ferguson, *supra* note 27, at 1283–84.

92. Steve Johnson, *Internet of Things Will Transform Life, but Experts Fear for Privacy and Personal Data*, SAN JOSE MERCURY NEWS (Nov. 1, 2014, 1:19 PM), http://www.mercurynews.com/business/ci_26845396/in [https://perma.cc/4CJA-NZHW] ("Even when designed for limited functions, experts say, many of these Web-linked gadgets will record whatever they see and hear in homes, which could provide detailed dossiers on the people living there, especially when combined with what's amassed by other interconnected machines. The personal data revealed could include everything from your friends, hobbies and daily routines to your political views, religious affiliation and even your sexual activities.").

93. Andrew Guthrie Ferguson, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards*, 66 OKLA. L. REV. 831, 836 (2014) (detailing the problems of aggregation in big data).

94. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 62 (2013) (discussing the issues of magnification).

95. This phenomenon has been called the mosaic theory. *See*, *e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012); Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 692 (2014).

96. There is a technological limitation to this surveillance, since current Wi-Fi sniffing devices are limited to a range of several hundred feet. Wi-Fi extenders, however, may make this technological limitation less important in the future.

97. *See*, *e.g.*, Hosein & Palow, *supra* note 82, at 1080 ("Rather than conducting searches of computers and mobile phones upon seizure, through the use of surveillance backdoors and vulnerabilities the users of these technologies are able to gain access to a device, whether a computer or a smartphone, through surreptitious means, often at a distance.")

law enforcement to secretly collect data.[98] Again, putting aside the statutory and constitutional limitations,[99] International Mobile Subscriber Identity (IMSI) catchers like the "Stingray" device can collect phone data by fooling cellphones into thinking the catchers are cell towers.[100] Using rather simple tools, researchers have already successfully hacked into Fitbit devices and obtained personal data.[101] Certain cars can be monitored and even remotely controlled through wireless signals.[102] Entire businesses are being developed to identify individual smartphones through wireless signals and then market

98. Voigt, *supra* note 85, at 541 ("Collecting private information from these unsecured networks is easier than the average consumer might believe. Many hackers use packet-sniffing technology, which can unveil the contents of unencrypted network transmissions, to illegally break into networks and capture data including passwords, IP addresses, and other information that will help an attacker infiltrate the network."); *see also* Mason, *supra* note 86, at 1159 ("Wi-Fi networks are either encrypted or unencrypted. Network owners commonly forgo encryption for a variety of reasons, such as to foster public access to information, lack of technological expertise, and the fact that users must affirmatively enable mechanisms to ensure encryption.").

99. While beyond the scope of this Article, an interesting question exists about the status of statutory protections for this wireless information under any of a number of federal privacy or computer statutes. *See generally* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 487 & n.2 (2013) ("The United States Code currently contains over twenty separate statutes that restrict both the acquisition and release of covered information. . . . Yet across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms.").

100. Hosein & Palow, *supra* note 82, at 1085–86 ("IMSI catchers and mobile interception devices make it possible for the government directly to monitor mobile communications without having to involve the carriers."); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 142–43 (2014) ("This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as 'IMSI catchers,' is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier.").

101. *See, e.g.*, Paul, *BitDefender Finds Phone to Smart Watch Communications Easy to Snoop*, SECURITY LEDGER (Dec. 10, 2014, 2:06 PM), https://securityledger.com/2014/12/bitdefender-finds-phone-to-smart-watch-communications-easy-to-snoop [http://perma.cc/5QX5-VBJB] ("Researchers from the security firm BitDefender have found that it is possible to snoop on wireless communications sent between smart watches and Android devices to which they are paired."); Peppet, *supra* note 32, at 134 & n.294 ("A team from Florida International University showed that the Fitbit fitness tracker could be vulnerable to a variety of security attacks, and that simple tools could capture data from any Fitbit within 15 feet.") (citing Mahmudur Rahman et al., Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device 1 (Apr. 20, 2013) (unpublished manuscript), http://arxiv.org /abs/1304.5672 [http://perma.cc/8W4D-6DBA]).

102. As has been described in tests, the electrical systems in cars can be taken over by hackers. *See Home, Hacked Home*, ECONOMIST (July 12, 2014, 2:59 PM), http://www.economist.com /news/special-report/21606420-perils-connected-devices-home-hacked-home [http://perma.cc/D8YN-WHYU] ("Modern cars are essentially a collection of computers on wheels, packed with many microcontrollers that govern their engines, brakes and so forth. Researchers . . . have shown that it is possible to hack into these systems and take over a vehicle.").

personalized ads and services to the consumer.[103] The opt-in nature of these convenience-focused services means that consumers will become open data sources to the sensors around them.[104] Yet many consumers may not even know they possess objects that are revealing information about their personal lives.[105] Further, the ubiquity of the sensors comes with the cost that many such sensors are designed cheaply without robust security measures.[106] Whether a function of consumer choice, ignorance, or technological vulnerability, IoT devices broadcast a secret pattern of life activities without much protection.[107]

Finally, while beyond the scope of this Article, IoT data trails provide the potential for a different sort of predictive surveillance.[108] The Internet of Things threatens to become a sentient force in the lives of consumers. Your refrigerator will order milk before you run out.[109] Lights in your house will turn on before you enter the room, and turn off when you leave. These micro-patterns (of what you did) will grow into larger and more sophisticated predictions about your future macro-patterns (what you will be doing).[110]

---

103. *See* Derek McAuley, *Century-Old Snooping: How World War I Code Breakers Taught Your Gas Meter to Snitch on You*, SLATE (Aug. 7, 2014, 7:57 AM), http://www.slate.com/articles/technology/future_tense/2014/08/what_wwi_code_breakers_and_hedy_lamarr_have_to_do_with_the_internet_of_things.html [http://perma.cc/HR23-CEP4] ("[W]ith many modern smartphone apps using push technology to continually synchronize with their servers in the cloud, and the phones in regular communication via your home Wi-Fi network when they are in range, detecting when a smartphone has left the building is a trivial matter.").

104. King, *supra* note 83, at 140–41 ("The wireless nature of RFID technology presents a security risk for consumers because they may be unaware that their personal information has been stolen through skimming or eavesdropping.").

105. *See, e.g.*, *id.* ("Skimming describes a situation in which someone with an unauthorized RFID-reader uses it to obtain information from an RFID chip in a mobile phone without the mobile phone user's knowledge or consent. Eavesdropping occurs when an 'unauthorized individual intercepts data as it is read by an authorized RFID-reader or transponder.'"); Peppet, *supra* note 32, at 140 ("Internet of Things devices are often small, screenless, and lacking an input mechanism such as a keyboard or touch screen. A fitness tracker, for example, may have small lights and perhaps a tiny display, but no means to confront a user with a privacy policy or secure consent.").

106. Nicole A. Ozer, *Rights "Chipped" Away: RFID and Identification Documents*, 2008 STAN. TECH. L. REV. 1, 7 (discussing the security risks of RFID technology).

107. *See, e.g.*, Sue Halpern, *The Creepy New Wave of the Internet*, N.Y. REV. BOOKS (Nov. 20, 2014), http://www.nybooks.com/articles/2014/11/20/creepy-new-wave-internet [https://perma.cc/KMJ5-XWBL] ("More recently, a study of ten popular IoT devices by the computer company Hewlett-Packard uncovered a total of 250 security flaws among them. As Jerry Michalski, a former tech industry analyst and founder of the REX think tank, observed in a recent Pew study: 'Most of the devices exposed on the internet will be vulnerable. They will also be prone to unintended consequences: they will do things nobody designed for beforehand, most of which will be undesirable.'").

108. Ferguson, *supra* note 88, at 383.

109. RUTLEDGE ET AL., *supra* note 42.

110. Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 211–12 (2014); Peppet, *supra* note 32, at 90 ("Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through 'Big Data' analytics, these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities.").

In the criminal context, these suspicious correlations might be the basis of further criminal investigation.[111] As I have written elsewhere, regular trips to the local drug store to purchase certain household items (which also happen to correlate with manufacturing methamphetamine) or unusual electricity usage (that might correlate with growing marijuana) could soon turn into actionable criminal suspicion.[112]

While perhaps unsettling, new sensor-based, object-based tracking should not be surprising. The drive for innovation, consumer efficiency, and self-awareness has turned ordinary activity into valuable data. Because of this valuable data, more and more "things" are being created to collect that information. The proliferation of smart objects brings with it the proliferation of advanced surveillance capabilities, a reality that statutory or constitutional law will soon need to address.[113]

C. Definitional Questions about the Internet of Things

To understand the subsequent constitutional arguments, which turn on the definition of a Fourth Amendment "effect," it is important to establish some working definitions of IoT technology. First, what is a "thing" for purposes of the Internet of Things?[114] Take as an example, a license plate affixed to an ordinary car.[115] As a stamped metal rectangle, it is a plain old "dumb" object: sitting in a garage, it reveals nothing but its physical form. Tagged with an RFID chip, it becomes a smart device able to communicate its location and reveal its identity. The RFID chip communicates the plate's existence and location through a readable sensor in a one-way communication. One could, thus, define a "thing" in the Internet of Things as any object that includes a unique identifier and transfers data using sensor technology.[116] Or, if one added a GPS transponder to the license plate this would add a level of interoperability such that the GPS transponder is communicating with the technology tracking

111. *See* Ferguson, *supra* note 88, at 383.

112. *See, e.g.*, Ferguson, *supra* note 93, at 861.

113. *See, e.g.*, James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 111 (1997); Voigt, *supra* note 85 (describing insufficient statutory protection for unsecured wireless data).

114. *See* Kominers, *supra* note 39, at 6 ("[The IoT] can mean a grand vision of sensors, information transmitters, and other devices being built into anything and everything to fundamentally change the way we interact with the world. Alternatively, it can mean nothing more than RFID chips being attached to our coffee mugs to improve the experience of going to coffee shops. It can mean open systems that anyone can enter or contribute to, or it can mean a finite, closed network to accomplish a discrete purpose.").

115. *See* RUTLEDGE ET AL., *supra* note 42.

116. *See* Gerd Kortuem et al., *Smart Objects as Building Blocks for the Internet of Th*ings, 14 IEEE INTERNET COMPUTING 44, 44 (2010), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5342399 [http://perma.cc/V7FF-PYRN] ("[Smart objects] sense, log, and interpret what's occurring within themselves and the world, act on their own, intercommunicate with each other, and exchange information with people.").

it.[117] You would not need to drive past an RFID sensor because the GPS reveals the location via real-time satellite technology.[118] Some definitions of the IoT would require this higher level of interoperability to qualify as being a part of the IoT.[119] But, even if not stamped with an RFID or GPS chip, because the license plate is uniquely identifiable through cameras or license plate reading technology it can become a part of a larger network of information sharing. Intriguingly, because an otherwise dumb object with no sensor or signal can still be identified by an appropriate sensor or camera, it too could be considered part of the Internet of Things. This identifiability raises the first definitional puzzle: clearly the RFID license plate and the GPS license plate should be thought of objects in the IoT, but should the otherwise ordinary, readable license plate also be included?[120]

For purposes of this Article the types of "things" that will be analyzed are actual things with communicating ability to other sensors. Old-fashioned dumb license plates would fall outside that definition. They are things, but not in the Internet of Things as defined here. Sensor-embedded license plates, however, would be included in the definition. The key components for purposes of this Article are (1) an identifiable object (2) that wirelessly communicates information about the object and (3) is linked to sensors that read information about the object. This excludes observational sensing devices (cameras, readers, scanners, etc.) from the Internet of Things but covers the smart objects themselves that are relaying data to collecting sensors.

Having addressed the types of "things" covered, the second definitional question becomes what constitutes the "thing" in the Internet of Things. Is it just the physical object? Is it also the stored electronic data in the object? Does it include the communication signals from the object to outside sensors? Could it cover the entire connected sensor network linking all such objects? In many ways, this is the key question of this Article, and requires both a technological and constitutional answer.

---

117. *See* Kominers, *supra* note 39, at 4 ("Devices will need to be capable of both communication (physically transferring data) and understanding (making sense of the data they receive). And this requires, at a minimum, substantial interoperability on the technical and data layers.").

118. For more information on GPS technology, see *Frequently Asked Questions*, GPS.GOV, http://www.gps.gov/support/faq (last visited Mar. 28, 2016).

119. *See* Kominers, *supra* note 39.

120. Peter Swire and other researchers at the Georgia Institute of Technology proposed reconceptualizing the Internet of Things as "the Internet of Devices." They define devices as "technologies that collect data or interact with their environment, and differentiate them from 'things,' which refers to objects about which data is collected." Under their framework, an untagged license plate is a thing, an RFID-tagged license plate is both a thing and a device, and the surveillance technologies that can read both types of license plates is a device. For technologists studying the security and privacy interests in devices, this broader definition is superior. After all, why exclude devices that convey the same identifying information because of a narrow definition of a "thing"? *See* RUTLEDGE ET AL., *supra* note 42.

Those designing smart technology rarely ask such definitional questions. An "enchanted" object is plainly not the same as an ordinary object. A "smart" pill bottle that reminds you to take your medicine is—by its very design—not an ordinary pill bottle.[121] The plastic container may be the same, but the "thing" is different. A consumer purchases a smart pill bottle precisely for its technology; therefore, the data recorded, the signals sent, and the integration with the consumer's health plan are all part of the product itself. Thus, if asked what part of the object should be considered a "thing" in the IoT, a technologist's answer would likely be, "all of it."

As discussed in this Article, because this answer has serious constitutional consequences, a more careful analysis may be necessary. While intended to be "smart," the object does not have to utilize its high-tech capabilities. For example, one might have bought the smart pill bottle because of its advanced pill tracking capabilities, but it can still be used as an ordinary pill bottle. The same is true for most smart objects. The object can be separated from its data or communicating functions. Thus, from a technological point of view, one could consider the "thing" as (1) merely the physical object; (2) the physical object and the digital data embedded in the object; (3) the physical object, digital data, and communication signals emanating from the object; (4) the physical object, digital data, communication signals, and the networked sensor system; or (5) the physical object, digital data, communication, networked sensor system, and the data on third-party systems.

This Article approaches the definitional problem from a "thing-based" perspective, and asks how smart things with embedded and communicating data fit within the Fourth Amendment. One could just as easily approach the same problem from a "data-centered" perspective analyzing the function, form, or location of the data itself. As I discuss in a companion article,[122] the data sent to the pharmacy from the enchanted pill bottle could be considered "papers" similar to a prescription, or a medical record. Or, because it is health information coming from a home, the Fourth Amendment's protection of "homes" could cover the data. This Article, however, focuses on redefining the thing itself, which necessitates redefining Fourth Amendment effects.

II.
FOURTH AMENDMENT EFFECTS AND THE INTERNET OF THINGS

The Fourth Amendment, of course, did not envision the Internet of Things. In a preelectricity, pretelephone era, the idea that things (or even people) could communicate wirelessly, instantaneously, and automatically did not enter into the calculation of drafting fundamental protections. Individuals

121. *See, e.g.*, Rose, *supra* note 4, at 9 (describing the GlowCap as an "enchanted" object).

122. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. (forthcoming 2016).

owned property, including personal effects that were tangible and quite ordinary.[123] Protecting that property from unreasonable searches and seizures made sense along with other protected interests of houses, persons, and papers.[124]

This Part briefly describes the original understanding of Fourth Amendment "effects" and its subsequent application in modern case law. Most recently, the Supreme Court—in *United States v. Jones*[125] and *Riley v. California*[126]—has addressed how new technologies impact Fourth Amendment effects. After this brief overview, the Part examines how the Internet of Things alters the constitutional analysis of effects. Using a hypothetical police surveillance of existing IoT devices, this Part reveals the gaps in the current doctrine in order to inform a new, expanded definition of "effects."

A. A Brief History of Fourth Amendment "Effects"

The term "effects" in the Fourth Amendment has long been understood to signify the protection of personal property.[127] At the time of the founding, people generally possessed two types of wealth: real property (land) and personal property (things). While some English jurists had once defined effects to include both real and personal property,[128] over time the accepted American understanding was that effects only signified the protection of the latter category.[129] As the Supreme Court stated in *Oliver v. United States*, "The

123. In addition to ordinary, effects were also quite limited. The standard of living in colonial America remained rather low, so most people did not have a great number of things. Basics such as pottery, furniture, gun parts, clocks, looking glasses, lamps, and clothing were found in colonial houses. *See, e.g.*, IVOR NOËL HUME, A GUIDE TO THE ARTIFACTS OF COLONIAL AMERICA 28–30 (1969).

124. *See* Hoffa v. United States, 385 U.S. 293, 301 (1966) ("What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile. There he is protected from unwarranted governmental intrusion. And when he puts something in his filing cabinet, in his desk drawer, or in his pocket, he has the right to know it will be secure from an unreasonable search or an unreasonable seizure.").

125. 132 S. Ct. 945 (2012).

126. 134 S. Ct. 2473 (2014).

127. *See* Oliver v. United States, 466 U.S. 170, 177 (1984).

128. *See, e.g.*, Doe v. Dring, 105 Eng. Rep. 447, 451 (K.B. 1814) ("'Effects is a very large and general term, and is confined to no particular description of property either in specie or value.' In its etymology it is derived from efficio, to accomplish, and means such things which a man has gained or acquired, and, in a more general sense, which he hath; it is synonimous with a man's substance, or all he is worth; and a devise of all he is worth has been held per se to pass the real estate."); *id.* ("So in *Hogan* v. *Jackson* Lord Mansfield took effects to be synonimous with worldly substance, which, he said, meant whatever could be turned to value; and therefore real and personal effects meant all a man's property.").

129. *Id.* at 458 ("But the subsequent cases of *Camfield v. Gilbert*, and *Doe v. Lainchbury*, have treated it otherwise, and as applying only to personalty in its primary signification."); *see* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 984 (2016) (noting the Federal Farmer as the only Anti-Federalist publication that

Framers would have understood the term 'effects' to be limited to personal, rather than real, property."[130]

This difference was important to the drafting of the Fourth Amendment. James Madison originally proposed that the Fourth Amendment protect "persons," "houses," "papers," and "*their other property*."[131] The language of "other property" was replaced with "effects" by the House Committee of the Eleven charged with revising the draft of the Constitution.[132] The modification was the only substantive change made to Madison's original language, and it was modified without explanation.[133]

Scholars have speculated that the change signified a narrowing (or clarifying) of the scope of protection to possessions in one's home, as opposed to possessions located in commercial properties or real property.[134] As Professor Thomas Davies summarized:

---

mentioned effects) (citing *No. 4*, FED. FARMER (Oct. 25, 1787), *reprinted in* 2 THE COMPLETE ANTI-FEDERALIST 262 (Herbert J. Storing & Murray Dry eds., 1981)); *see also Doe*, 105 Eng. Rep. at 449 ("In *Camfield v. Gilbert*, and *Doe v. Lainchbury*, it was taken for granted that effects in its natural signification imports personal effects."); Brady, *supra*, at 984, (recognizing that "[n]o state constitution included the word [effects], nor did any of the proposals from state-convention members").

130. *Oliver*, 466 U.S. at 177 n.7 (1984) (citing *Doe*, 105 Eng. Rep. at 449 (discussing prior cases)); 2 WILLIAM BLACKSTONE, COMMENTARIES *16, *84–85; *see also* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 690–98 (2009).

131. Madison's first draft of the Fourth Amendment read:

> The rights of the people to be secured in their persons, their houses, their papers, and *their other property*, from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be seized.

See NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 100 n.77 (1937) (citing 1 ANNALS OF CONG. 452).

132. David E. Steinberg, *The Original Understanding of Unreasonable Searches and Seizures*, 56 FLA. L. REV. 1051, 1077 (2004) ("[A] House of Representatives Committee changed the phrase 'and their other property,' to the narrower language 'effects.'") (citing *House Committee of Eleven Report*, July 28, 1789, *reprinted in* THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 223-24 (Neil H. Cogan ed., 1997)).

133. *Oliver*, 466 U.S. at 176–77; Altman v. City of High Point, 330 F.3d 194, 201 (4th Cir. 2003) ("Because there are no records of the Committee's deliberations, it is unclear precisely why that change was made."); Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1048 (2011) (recognizing that the House Committee of Eleven edited Madison's draft stating, "the sole substantive change being a narrowing of the objects protected from 'other property' to 'effects'").

134. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 710–11 (1999) ("Because 'effects' was usually understood to designate moveable goods or property (but not real property or premises), the most likely explanation for the substitution is that the Committee intended to narrow the scope of interests protected by Madison's proposal."); *see id.* at 711 ("Thus, the Committee's formulation implied that 'houses' were the only type of premises protected by the right to be secure, although 'effects' denoted that any type of items or goods that might be located within a house, including commercial goods, were also protected. A plausible motive for adopting a narrower expression regarding the scope of protection is patent: customs collections would be the primary source of revenue for the new government, and the Committee may have been reluctant to adopt an inflexible constitutional protection that would limit legislative authority to provide for

> In sum, although the evidence on this point is less than definitive, the available linguistic and statutory evidence suggests that "persons, houses, papers, and effects" was understood to provide clear protection for houses, personal papers, the sorts of domestic and personal items associated with houses, and even commercial products or goods that might be stored in houses—while leaving commercial premises and interests otherwise subject to congressional discretion.[135]

Since that initial change, courts have interpreted Fourth Amendment effects to cover all of an individual's personal property with a general view that "effects" means goods,[136] moveable objects,[137] or possessions.[138]

The Supreme Court has explicitly referenced certain objects as "effects" throughout its history, including containers,[139] packages held by a person,[140] packages given to private carriers,[141] footlockers,[142] automobiles,[143] as well as a variety of contraband recovered in criminal cases. State and federal courts have

---

searches of commercial premises—especially given that the popular concern regarding searches focused on violations of houses.").

135. *Id.* at 714.

136. *Id.* at 708 n.461 ("'Effects' does not seem to have been defined in framing-era legal dictionaries, but it was defined in general purpose dictionaries. A 1730 dictionary defined 'effects' as 'the goods of a merchant, tradesman, &c.' Johnson's Dictionary, (published in 1755), defined the plural of 'effect' simply as 'Goods; moveables.'") (internal citations omitted).

137. *Altman*, 330 F.3d at 201 ("By contrast, 'effects' referred only to personal property, and particularly to goods or moveables."); *see* DICTIONARIUM BRITANNICUM (Nathan Baily ed., 1730) (defining "effects" as "the goods of a merchant, tradesman, & c"); 1 NOAH WEBSTER, AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE (1828) (defining "effect" as "[i]n the plural, effects are goods; moveables; personal estate").

138. State v. Davis, 929 A.2d 278, 295–96 (Conn. 2007) ("In other words, we do not perceive any meaningful distinction between 'effects' and 'possessions.'"); People v. Smith, 360 N.W.2d 841, 849 (Mich. 1984) ("The terms 'possessions' and 'effects' are virtually identical in meaning and are often used interchangeably.").

139. Florida v. Jimeno, 500 U.S. 248, 253 (1991) ("Luggage, handbags, paper bags, and other containers are common repositories for one's papers and effects, and the protection of these items from state intrusion lies at the heart of the Fourth Amendment.").

140. *See* Walter v. United States, 447 U.S. 649, 654 (1980); *Ex parte* Jackson, 96 U.S. 727, 733 (1877); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 n.14 (2009) ("The court has also confirmed that sealed packages given to private carriers are Fourth Amendment 'effects' in which the public has a 'legitimate expectation of privacy' vis-a-vis the government."). *See generally* Rios v. United States, 364 U.S. 253 (1960).

141. United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("When the wrapped parcel involved in this case was delivered to the private freight carrier, it was unquestionably an 'effect' within the meaning of the Fourth Amendment. Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable.").

142. United States v. Chadwick, 433 U.S. 1, 12 (1977).

143. Cady v. Dombrowski, 413 U.S. 433, 439 (1973) ("Although vehicles are 'effects' within the meaning of the Fourth Amendment, 'for the purposes of the Fourth Amendment there is a constitutional difference between houses and cars.'"); Brinegar v. United States, 338 U.S. 160, 182, (1949) ("His automobile was one of his 'effects,' and hence within the express protection of the Fourth Amendment.") (cited by Chambers v. Maroney, 399 U.S. 42, 52 (1970)).

even recognized such unusual things as apiaries (beehives)[144] and dogs[145] to be effects for purposes of the Fourth Amendment. Even though the definition of effects has expanded, scholars have begun to suggest that effects may need a broader definition in the digital age to cover computers, flash drives, and other digital storage devices.[146] As it currently stands, however, effects have remained simple, unenchanted objects. The next Section examines two recent Supreme Court cases focused on technology and Fourth Amendment effects, which have attempted to respond to this changing reality.

B. The Modern Fourth Amendment

Scholars who study the Fourth Amendment agree that new technologies have created some fascinating and largely unanswered doctrinal puzzles.[147] While technology has always been a driver in Fourth Amendment development, new mass surveillance capabilities are growing in scope and sophistication.[148] Two significant doctrinal issues have arisen in recent cases involving police investigation with new technologies. In *United States v. Jones*, the Supreme Court resurrected a more property-based conception of the Fourth Amendment centered on the minor physical intrusion of placing a GPS transponder on a personal effect (a car).[149] In *Riley v. California*, the Supreme Court addressed the digital and communications capabilities of our most

144. Allinder v. Ohio, 808 F.2d 1180, 1186 (6th Cir. 1987) ("Apiaries are commercial property. They are also personal property since they are movable and at times are moved for rental to farmers in crop pollination. As such they fall within the definition of effects.").

145. *See* Brown v. Muhlenberg Twp., 269 F.3d 205, 209–10 (3d Cir. 2001) (holding that dogs are "effects"); Fuller v. Vines, 36 F.3d 65, 68 (9th Cir. 1994) (same); Lesher v. Reed, 12 F.3d 148, 150–51 (8th Cir. 1994).

146. Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 51 (2013) ("Portable devices like cellphones and flash drives are 'effects' subject to search and seizure like briefcases and backpacks."); Richard Sobel et al., *The Fourth Amendment Beyond* Katz, Kyllo *and* Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 8 (2013).

147. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 71 (2005); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506–07 (2007); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1321–22 (2002); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1397–98 (2002).

148. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004); Rushin, *supra* note 66, at 287–89; Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1383 (2004).

149. 132 S. Ct. 945, 949 (2012) ("Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century."). *But see* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67 (arguing that trespass did not control early Fourth Amendment cases).

ubiquitous enchanted object—the smartphone.[150] Both cases provide a window into the Fourth Amendment's past and an opening to its future. These cases also provide the framework to understand how the Fourth Amendment currently addresses smart objects.

1. United States v. Jones

Much has already been written about *Jones* because the case represented an unexpected return to a Fourth Amendment theory largely ignored for more than fifty years.[151] *Jones* presented the issue of whether "attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[152] The case concerned the continuous GPS surveillance of Antoine Jones for twenty-eight days as a result of a large-scale drug distribution investigation.[153]

Prior to *Jones*, the Court's Fourth Amendment analysis would have only examined whether the ongoing police surveillance violated Mr. Jones's reasonable expectation of privacy.[154] This legal standard derived from *Katz v. United States*,[155] the seminal modern search case that required an analysis of whether the government violates a subjective expectation of privacy that society recognizes as objectively reasonable.[156] While concurring Justices in *Jones* adopted this reasonable expectation of privacy approach, the majority opinion relied on a different line of reasoning.

The majority focused on the physical search of the effect (the car), holding "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"[157] Justice Scalia wrote:

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of

150. 134 S. Ct. 2473 (2014); Adam Lamparello & Charles MacLean, Riley v. California*: The New* Katz *or* Chimel*?*, 21 RICH. J.L. & TECH. 1, 4 (2014).

151. *See, e.g.*, Thomas K. Clancy, United States v. Jones*: Fourth Amendment Applicability in the 21st Century*, 10 OHIO ST. J. CRIM. L. 303 (2012); Caren Myers Morrison, *The Drug Dealer, The Narc, and the Very Tiny Constable: Reflections on* United States v. Jones, 3 CALIF. L. REV. CIRCUIT 113 (2012); Erin Murphy, *Back to the Future: The Curious Case of* United States v. Jones, 10 OHIO ST. J. CRIM. L. 325 (2012).

152. *Jones*, 132 S. Ct. at 948.

153. *Id.*

154. *See* United States v. Karo, 468 U.S. 705, 729 (1984); United States v. Knotts, 460 U.S. 276, 276 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."); Richard H. McAdams, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 317–35 (1985).

155. 389 U.S. 347 (1967).

156. *Id.* at 361 (Harlan, J., concurring). *Katz* involved the interception of a telephone call from an enclosed, public phone booth.

157. *Jones*, 132 S. Ct. at 949.

> obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.[158]

Because an "effect"—the car—had been physically intruded upon (by placing the GPS device on the object), there was a constitutionally significant interference with Mr. Jones's Fourth Amendment rights. Justice Scalia cited "the Fourth Amendment['s] . . . close connection to property," referencing famous English cases involving the sacred nature of property rights,[159] and reminded the Court that "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[160] Justice Scalia acknowledged the prevailing *Katz* approach, but contrary to the general consensus among scholars and judges, asserted that the property-based approach has always remained an available basis for decision (just not one relied on since *Katz* was decided).[161] Because the case could be decided on narrower, property-focused grounds, Justice Scalia opted for this alternative rationale.

The concurring Justices—Justice Sotomayor writing for herself and Justice Alito writing for four others—all agreed that a Fourth Amendment search had occurred, but on different grounds.[162] Justice Sotomayor accepted Justice Scalia's property-based rationale, but also opined that such long-term surveillance would violate a reasonable expectation of privacy. As Justice Sotomayor reframed the question, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[163] She broadly articulated the dangers of high-tech surveillance that cannot only track, but aggregate data about individuals.[164] Additionally, Justice Sotomayor called into question the

158. *Id.*

159. *Id.* ("[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law.") (citing Entick v. Carrington, 95 Eng. Rep. 807, 817 (C.P. 1765)).

160. *Id.*

161. Justice Scalia's assertion belies the history and general discussion of the issue, which has long left the *Olmstead* line of cases in the graveyard of Fourth Amendment history. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928) (holding that wiretapping was not an impermissible search or seizure under the Fourth Amendment because there was no physical trespass or confiscation); Peter P. Swire, Katz *is Dead. Long Live* Katz., 102 MICH. L. REV. 904, 905 (2004); Kerr, *supra* note 147; David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 158 (2002).

162. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring); *see id.* at 957 (Alito, J., concurring).

163. *Id.* at 956 (Sotomayor, J., concurring).

164. *Id.* at 955–56 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

existing third-party doctrine, which provides no protection to information shared with third parties.[165] While focused on the problem of GPS tracking, in particular, the privacy concerns articulated in her concurrence plainly impacts other surveillance technologies.

Justice Alito offered a sharp critique of Justice Scalia's "18th century tort" approach to modern surveillance concerns.[166] Not only did Justice Alito find that the *Katz* standard could resolve the question at issue, but he also stated that Justice Scalia's property-focused approach ignored the harder questions of nontrespassory surveillance technologies.[167] He concluded, "Relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[168] Unfortunately, Justice Alito did not provide much guidance about how to define short- or longer-term monitoring, or what offenses would be covered. In Antoine Jones's case, the twenty-eight days of monitoring was sufficient to find a violation of a reasonable expectation of privacy.[169]

Five significant conclusions can be drawn from *Jones*. First, "constitutionally protected interests" involving persons, houses, papers, and effects are once again central to any Fourth Amendment analysis. Second, the long-dormant property-based physical intrusion theory of the Fourth Amendment has been resurrected. Third, five Justices believe that the reasonable expectation of privacy test can be applied to some nonphysical technologically based surveillance. Fourth, five Justices believe extensive collection and aggregation of personal data through technological means requires some constitutional protection. Fifth, at least one Justice is concerned about the reach of the third-party doctrine.

Each of these conclusions impacts how an Internet of Things sensor-based system should be analyzed. First, smart objects (as effects) should be considered among other recognized constitutionally protected interests. In addition, these smart effects can be physically intruded upon to obtain personal digital information. Similarly, nonphysical surveillance of these smart objects raises difficult reasonable expectation of privacy questions. Finally, the

165. *Id.* at 957 ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."). *See generally* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1015 (2007); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 (2006); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009).

166. *Jones*, 132 S. Ct. at 957–58 (Alito, J., concurring).

167. *See generally id.* at 957–64.

168. *Id.* at 964.

169. *Id.* ("I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.").

problems of aggregation and the third-party doctrine are implicated with the collection of personal information from these smart devices. In short, the questions arising from *Jones* are reflected and complicated in a world governed by the Internet of Things.

2. Riley v. California & United States v. Wurie

At issue in *Riley* (and the companion case *Wurie*) was digital information recovered from a smartphone incident to arrest.[170] A phone—an effect—was recovered from two suspects after a search of each suspect's person.[171] The police obtained the information by physically exploring the phone to observe the data (text, photos, videos, contacts, etc.) through the normal operation of the phone.[172]

Riley is technically a "search incident to arrest" case that turns on the scope of the search *of the person* at the time of arrest. In one reading of the case, the Supreme Court merely applied the traditional line of search incident to arrest cases—*Chimel*,[173] *Robinson*,[174] and *Gant*[175]—and found that the digital information on a smartphone differed from physical evidence because concerns for officer safety and the potential destruction of evidence did not apply.[176] In this reading, the fact that the object is an "effect" is less relevant than the fact that the object was recovered on the person incident to arrest. While the Court undoubtedly engaged this analysis, it ran into logical difficulties because prior precedent had previously allowed all recovered objects to be searched incident to arrest.[177] As the Court admitted, "A mechanical application of *Robinson* might well support the warrantless searches at issue here."[178] To sidestep this precedent, the Court made the novel analytical move to differentiate physical objects from digital content (data) in those physical objects.[179] The physical object (the phone) could be searched to

170. Riley v. California, 134 S. Ct. 2473, 2480 (2014) ("These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.").

171. David Leon Riley and Brima Wurie (in a separate companion case) were both arrested and both had phones taken from their persons and searched incident to arrest. *See generally id.*

172. *Id.* at 2480–81.

173. Chimel v. California, 395 U.S. 752 (1969).

174. United States v. Robinson, 414 U.S. 218 (1973).

175. Arizona v. Gant, 556 U.S. 332, 350 (2009).

176. *Riley*, 134 S. Ct. at 2484–88 (discussing why the *Chimel* rationale does not apply to searches of smartphones recovered incident to arrest).

177. *Id.* at 2484.

178. *Id.*

179. *Id.* ("But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.").

ensure, for example, that a razor blade was not hidden inside, but the digital content could not be searched without a warrant.[180]

This shift in emphasis has profound implications for a Fourth Amendment analysis of smart effects. First, the Court implicitly creates a distinction between simple objects and smart objects (with data inside), with the latter being granted additional protection.[181] This distinction between physical objects and digital objects breaks new ground for the Supreme Court, opening the door to perhaps a different analysis for digital information. Second, since a warrant is required to search data on a phone incident to arrest, by implication a warrant would be required to search a phone without the legal authority of an arrest. Thus, in a future case when an officer seizes a phone before arrest, *Riley* implicitly forbids a warrantless search (absent an exigency).

Writing for the majority, Chief Justice Roberts, however, did not stop at merely distinguishing digital information from physical objects based on the officers' safety and destruction of property rationales in *Chimel* and prior cases. Instead, the Court specifically articulated the privacy considerations of smartphone data. In rather sweeping language, the Court addressed why data located in smart objects must be protected. First, the Court recognized that cellphone data differed both qualitatively and quantitatively from ordinary objects.[182] Quantitatively, the storage capacity of phones allowed a tremendous amount of information to be revealed.[183] In addition, there is also a qualitative difference in the data. Stored data reveals a person's interests, whereabouts, and sometimes thoughts in a way that a physical object could not.[184] Internet search and browsing histories, locational data, and even the type of news or reading material on a phone can create a composite picture of an individual's concerns and thoughts.[185]

Such acknowledgement of the privacy interests involved in data goes beyond smartphones. As Chief Justice Roberts recognized, a smartphone is really a misnomer as the thing at issue is a "minicomputer[]" with vast collection, networking, and consumer applications.[186] While *Riley* addressed the existing technologies of smartphones in 2014, the broader conclusions apply to any smart device that can track, collect, share, store, and process personal data about its owner. The difference between smartphones and devices

180. *Id.* at 2485 ("Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.").

181. *Id.* at 2484–85.

182. *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

183. *Id.*

184. *Id.* at 2490–91.

185. *Id.* at 2490 ("The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.").

186. *Id.* at 2489.

in the Internet of Things is one of degree, not kind. In time, even simple sensors will be quite sophisticated objects capable of communication and recording—and soon they will be part of a larger web of surveillance.

Finally, Chief Justice Roberts acknowledged that considering a smartphone merely as a container of stored digital information is largely a fiction, because the device is constantly communicating with stored information on the cloud.[187] The data may be on the actual phone, but it may also be somewhere else and thus, "[t]he possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson*."[188] The unanswered question, of course, is whether the data communicated from the smartphone to the cloud is protected in the same way as the data in the smartphone itself.[189]

The questions arising from *Riley* are currently unsettled. Digital information is different, but how different? In *Riley*, the police physically unlocked and looked through the phone; but what if they used technology to do virtually the same thing? What if they had just downloaded all the content onto a thumb drive to be searched later, after a warrant? Because the case arose under a search incident to arrest exception, the Court did not have to answer these harder questions.

In the world of the Internet of Things—a world of smart objects collecting and sharing personal information—these same questions must be confronted. The next Section attempts to apply the current Fourth Amendment doctrine to map the doctrinal gaps and address the challenges brought on by IoT technology.

C. Existing Fourth Amendment Doctrine Applied to the Internet of Things

This Section examines a hypothetical police investigation to demonstrate the difficult questions that arise as simple objects transition to "smart devices" in the Internet of Things. The goal is to provide an analytical framework under existing Fourth Amendment law and to expose the gaps in current doctrine. Adding complexity to the analysis, some effects will be found within other constitutionally protected areas—in homes, in cars, or on persons.[190] Existing Fourth Amendment doctrine provides some clear answers, some muddled

187. *Id.* at 2491 ("Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself.").

188. *Id.*

189. *See generally* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009); William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195 (2010).

190. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 513 (1971) (recognizing the analytical "difficulty [that] derives from the fact that effects enjoy derivative protection when located in a house or other area within reach of the Fourth Amendment").

answers, and many questions as applied to the types of IoT devices currently in use. This Section focuses on the constitutional issues, leaving aside various statutory limitations on police conduct.[191]

1. An IoT Criminal Investigation

Imagine in the near future, police wish to investigate a suspected drug dealer entirely through Internet of Things objects. Similar to the Antoine Jones investigation,[192] police seek to track a suspect's location throughout the day to link him to a stash of illegal narcotics. Police wish to search information from five sources: (1) the networked IoT appliance system that controls the suspect's home lighting, heating, and kitchen appliances (similar to a NEST system); (2) the IoT connected Fitbit band or running shoes that track how many steps and where the suspect walks; (3) the IoT navigation system in the suspect's car; (4) the suspect's smartphone; and (5) an RFID-equipped package that the suspect possesses. By tracking each object or system, police can determine when the suspect leaves his house, where he goes by car or by foot, his level of physical exertion, and—utilizing the smartphone—even routine daily activities.

These various "effects"—some located within other constitutionally protected areas—create analytically distinct Fourth Amendment problems. Each of these "effects," representing (1) effects in homes; (2) effects on persons; (3) effects in cars; (4) digital effects; and (5) pure effects, will be addressed in turn. And, as discussed above, analysis of each effect will need to incorporate questions about whether the Fourth Amendment protects the physical object, the digital data within the object, the communication signals from sensors in the effects, or the networked information held by a third party.

a. Investigating Effects Located in Homes

Monitoring a suspect's home is a common law enforcement technique. Whether by stakeouts or by surveillance cameras, police regularly track the movements of suspects in and out of their homes.[193] With the Internet of Things, however, police do not need to suffer in cramped cars drinking cold coffee. By monitoring IoT devices (including lighting or appliance use), police can now not only know whether a suspect is home, but also when he is cooking dinner, watching television, or getting ready for bed.[194] The constitutional

191. *See* Mani Potnuru, *Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 95–96 (2012). *See generally* Shaina Hyder, *The Fourth Amendment and Government Interception of Unsecured Wireless Communications*, 28 BERKELEY TECH. L.J. 937 (2013).

192. United States v. Jones, 132 S. Ct. 945, 949 (2012).

193. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001) (discussing stakeout with thermal imaging device); Commonwealth v. Williams, 431 A.2d 964, 966 (Pa. 1981) (holding that a nine-day stakeout using high-tech equipment, including night vision goggles, violated a reasonable expectation of privacy).

194. *See supra* Part I.

question is whether obtaining that information is a search for Fourth Amendment purposes, which, in turn, requires asking whether police obtained the information through physical intrusion-trespass (*Jones* test) or by violating a reasonable expectation of privacy (*Katz* test).

i. Physical Object & Embedded Data of Effects in Homes

Because IoT devices are located within a home, the question of direct physical removal of the data becomes fairly easy to resolve. The Fourth Amendment protects houses and effects, and a physical search of the home to view the appliance device (the physical object) would be a straightforward Fourth Amendment search.[195] If police entered the house without a warrant, you would have a physical invasion of the home that violated a reasonable expectation of privacy.[196] If police then physically touched the IoT device to download the data, you would have a trespass to the effect, and a violation of the expectation of privacy.[197] Just as police cannot enter your house and search a computer or look in your drawers without a warrant, the physical object and its data would be protected by both the houses and effects language of the Fourth Amendment.

ii. Communication Signals of Effects in Homes

A more difficult question arises if police had a device capable of intercepting—from outside the home—the wireless signals emanating from IoT devices within the home.[198] Police cannot see and do not touch the physical

195. Payton v. New York, 445 U.S. 573, 586 (1980) ("It is a 'basic principle of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable.").

196. *Id.* at 589–90 ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: 'The right of the people to be secure in their . . . houses . . . shall not be violated.' That language unequivocally establishes the proposition that '[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'").

197. The physical touching would suffice for trespass (or physical intrusion).

198. For examples of such devices arising from civilian and law enforcement technologies, see Cecilia Kang, *Growing Anger over Google Street View Privacy Breach*, WASH. POST. (May 20, 2010, 8:00 AM), http://voices.washingtonpost.com/posttech/2010/05/the_anger_is_growing_over.html [http://perma.cc/UGN3-HZEZ]; Kim Zetter, *DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls*, WIRED (Aug. 4, 2011, 2:13 PM), http://www.wired.com/threatlevel/2011/08/blackhat-drone [http://perma.cc/47UU-BMD7] (discussing the ability of drones to access wireless networks and intercept communications). In addition, intercepting wireless signals has been litigated in both criminal and civil contexts. *See*, *e.g.*, Joffe v. Google, Inc., 729 F.3d 1262, 1278–79 (9th Cir. 2013); United States v. Ahrndt (*Ahrndt II*), 475 F. App'x 656 (9th Cir. 2012); United States v. Ahrndt (*Ahrndt III*), No. 3:08-CR-00468-KI, 2013 WL 179326, at *11 (D. Or. Jan. 17, 2013) (criminal); *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1077–78 (N.D. Cal. 2011) (civil); *see also* Pell & Soghoian, *supra* note 100, at 146.

object or the data located on the device. Instead, they only collect the wireless data as it leaves the house and connects to an outside sensor.

Under the physical intrusion-trespass analysis applied in *Jones*, no Fourth Amendment search has been conducted. This is so because no physical invasion of physical property has occurred. Critics of Justice Scalia's narrow physical intrusion-trespass theory raised this concern and recognized that the theory would not protect from sophisticated technological snooping.[199]

Under a reasonable expectation of privacy test, however, this type of high-tech acquisition of information emanating from inside the house appears roughly analogous to the facts of *Kyllo v. United States*.[200] In *Kyllo*, the Court held that using a thermal imaging device to scan heat patterns of a private home was a search because it violated a reasonable expectation of privacy.[201] The device used by police was not commonly available to the public and potentially revealed personal details, including, for example, "at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate.'"[202] The dissent argued that no expectation of privacy should be provided to heat signals, because the technology only intercepted heat waves emanating from the house (i.e., the heat waves were *outside* of the house and thus not subject to Fourth Amendment protection).[203] The majority rejected this argument and protected the information because it *came from within* the house.[204] Similarly, in *Florida v. Jardines*, the Supreme Court found that the scent of marijuana emanating from the house was protected from capture by a trained police dog on the curtilage.[205] The concurring Justices found the use of a drug-sniffing dog directed at scents coming from the house violated an expectation of privacy.[206] By analogy, because the IoT communication signals originate from the home (even if captured outside the home), the Fourth Amendment should still protect them.

---

199. United States v. Jones, 132 S. Ct. 945, 959–61 (Alito, J., concurring) (criticizing the majority's reliance on trespass). Unless "effect" is defined as including the communications, and further that interception of the communications is a search or seizure (of signals), the Fourth Amendment would not apply.

200. 533 U.S. 27, 27 (2001).

201. *Id.* at 40.

202. *Id.* at 38. Technology through the Internet of Things might also reveal which room she took her bath, the water usage, the temperature in the room, and where she went before and after that moment of relaxation.

203. *See id.* at 43–44 (Stevens, J., dissenting) ("Thus, the notion that heat emissions from the outside of a dwelling are a private matter implicating the protections of the Fourth Amendment (the text of which guarantees the right of people 'to be secure *in* their . . . houses' against unreasonable searches and seizures) is not only unprecedented but also quite difficult to take seriously.") (alteration in original).

204. *Id.* at 35.

205. Florida v. Jardines, 133 S. Ct. 1409, 1417–18 (2013).

206. *Id.* at 1418 (Kagan, J., concurring) ("Was this activity a trespass? Yes, as the Court holds today. Was it also an invasion of privacy? Yes, that as well.").

Of course, the above discussion turns more on the Supreme Court's heightened protection of the home.[207] "At the very core" of the Fourth Amendment "stands [for] the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[208] Thus, for effects within homes the analysis of the Internet of Things largely overlaps. At least for investigations directed at a specific home, secured communication signals emanating from smart effects within that home would be protected under a reasonable expectation of privacy analysis.[209]

The only remaining question is what should happen to communications emanating from home IoT devices that are captured at some distance from the home. Perhaps the wireless signals are routed through several servers, or intercepted just before entering the third-party provider's network.[210] This could conceivably occur in a different jurisdiction.[211] Is the communication signal still part of the effect? Is it separate from the effect? Has it been severed from the effect? Under existing Fourth Amendment law, there is no clear answer. Obtaining these signals would not be a physical invasion (no trespass), and with the exception of *Kyllo*, the Supreme Court has not addressed whether individuals have a reasonable expectation of privacy in such signals detailing home appliance usage outside the home. Such information reveals a personal pattern of family and home habits and is likely more personal than Charlie Katz's phone conversation for which police would need a warrant, but there is no clear answer. As will be discussed, this Article argues that such communications can be considered part of a redefined effect, and interference with those communications could be considered a search for Fourth Amendment purposes.

---

207. *See, e.g.*, Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 940 (2010).

208. *Jardines*, 133 S. Ct. at 1414 ("[W]hen it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

209. This question has not been resolved. *See also* Hyder, *supra* note 191, at 950–52 (describing splits among courts). *Compare* United States v. Soderholm, No. 4:11CR3050, 2011 WL 5444053, *4 (D. Neb. Nov. 9, 2011), *with* United States v. Ahrndt, 475 Fed. Appx. 656 (9th Cir. 2012).

210. *See supra* note 165 and accompanying text (discussing the third-party doctrine); Riley v. California, 134 S. Ct. 2473, 2484–88 (2014) (discussing why the *Chimel* rationale does not apply to searches of smartphones recovered incident to arrest).

211. The range of a typical indoor Wi-Fi device currently is much more limited (about 150 feet). Bradley Mitchell, *What is the Typical Range of a Typical Wi-Fi Network?*, ABOUT TECH, (Mar. 18, 2014) http://compnetworking.about.com/cs/wirelessproducts/f/wifirange.htm [http://perma.cc/9GEL-TNW5].

iii. Networked Information of Effects in Homes

The Fourth Amendment does not currently protect information shared with third parties—including commercial third parties.[212] If police investigators wanted to obtain the data provided by the suspect's IoT household appliances directly from the company contracted to monitor those appliances, the police could do so without much Fourth Amendment difficulty.[213] Just as police can request electricity usage data from the electrical company,[214] police can request the same data from the third-party provider of the IoT system.[215] Under existing constitutional law, there are no explicit protections for IoT device information and thus, traditional third-party doctrine rules would apply.

Simply stated, if the police wished to monitor the house using IoT devices by requesting the data directly from the service provider, any Fourth Amendment objection would be unavailing. While scholars have expressed dissatisfaction with the third-party doctrine, and at least Justice Sotomayor has expressed interest in revisiting its application, the third-party doctrine remains good law.[216]

b. Investigating Effects Located on Persons

The proliferation of personal consumer items with IoT capabilities also creates opportunities for investigatory uses.[217] Clothing, jewelry, and bags—now termed "wearables"[218]—allow easy tracking, and some newer items even

212. *See supra* note 165 and accompanying text (discussing the third-party doctrine).

213. *Id.*

214. Dean Narciso, *Police Seek Utility Data for Homes of Marijuana-growing Suspects*, COLUMBUS DISPATCH (Feb. 28, 2011, 11:21 AM), http://www.dispatch.com/content/stories/local/2011/02/28/police-suspecting-home-pot-growing-get-power-use-data.html [http://perma.cc/YJ4W-WASC] ("At least 60 subpoenas are filed each month across the state seeking customers' energy-use records from American Electric Power and other utilities."); Matt Liebowitz, *Smart Electricity Meters Can Be Used to Spy on Private Homes*, NBC NEWS (Jan. 10, 2012, 4:03 PM), http://www.nbcnews.com/id/45946984/ns/technology_and_science-security/t/smart-electricity-meters-can-be-used-spy-private-homes [http://perma.cc/6PBU-RJGN] ("The researchers . . . intercepted the supposedly confidential and sensitive information, and, based on the fingerprint of power usage, were able to tell not only whether or not the homeowners were home, away or even sleeping, but also what movie they were watching on TV."). *See generally* Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 211 (2011).

215. Ferguson, *supra* note 93, at 861 (discussing third-party collection of records).

216. *See supra* note 165 and accompanying text.

217. Johnson, *supra* note 92; Lucas Mearian, *Data from Wearable Devices Could Soon Land You in Jail*, COMPUTERWORLD (Dec. 8, 2014, 3:00 AM), http://www.computerworld.com/article/2855567/data-from-wearable-devices-could-soon-land-you-in-jail.html [https://perma.cc/ZD23-KCYX].

218. Jennifer E. Smith, *You Can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J.L. & TECH. 249, 258–59 (2007) ("RFID has been used not just to track products, but also as an integral component of the product, from toys to automobiles to even jewelry."); Scott Stein, *Connected, Invisible and Everywhere: Wearables at CES Aimed to Blend In*, CNET (Jan. 8, 2015, 5:45 PM), http://www.cnet.com/news/invisible-and-everywhere-wearable-at-ces [http://perma.cc/857E-HNAU] (detailing the latest wearable devices at the 2015 Consumer Electronic Show).

include communication capabilities.[219] If, for example, our drug-dealing suspect wore fitness tracking shoes or a bracelet that connected him to a GPS data trail, police investigators might want access to that information. In a criminal prosecution, the fact that a suspect's car was parked in front of a narcotics stash house is good evidence.[220] The fact that the suspect got out of that car and walked into the stash house is even better evidence.

i. Physical Object & Digital Data

Generally, physical effects worn as clothing or accessories on persons are treated as part of the person for Fourth Amendment purposes.[221] In the same way a search of one's pants pocket is a search of a person, the physical search of a bracelet or shoe would be a Fourth Amendment search of a person.[222] Under both physical intrusion and reasonable expectation of privacy theories, the case law is clear that such physical investigation of things on the person is a search.[223] This reasoning would also hold for direct extraction of digital information from an item a suspect was wearing. Police could no more physically seize and download the data in a Fitbit bracelet than examine the contents of a wallet in a man's pocket without legal justification. The

219. Cory Weinberg, *A High-Tech New Way for Your Boss to Follow You Everywhere*, BLOOMBERG BUS. (Aug. 1, 2014, 4:55 PM), http://www.bloomberg.com/news/articles/2014-08-01/wearable-technology-will-let-companies-monitor-worker-productivity [https://perma.cc/RR6B-3UEV] ("Workplace-management software company Kronos says it is expanding its software offerings to work with wearables that have tracking and communication capabilities for manufacturing and retail companies.").

220. In the *Antoine Jones* case, the prosecution was limited to tracking the car as a mechanism to connect Mr. Jones to houses believed to play a role in the drug conspiracy. *See* United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

221. Wyoming v. Houghton, 526 U.S. 295, 303 n.1 (1999) ("This distinction between searches of the person and searches of property is assuredly *not* 'newly minted.' And if the dissent thinks 'pockets' and 'clothing' do not count as part of the person, it must believe that the only searches of the person are strip searches.") (internal citation omitted); *see id.* at 308 (Breyer, J., concurring) ("Purses are special containers. They are repositories of especially personal items that people generally like to keep with them at all times. So I am tempted to say that a search of a purse involves an intrusion so similar to a search of one's person that the same rule should govern both. However, given this Court's prior cases, I cannot argue that the fact that the container was a purse automatically makes a legal difference, for the Court has warned against trying to make that kind of distinction. But I can say that it would matter if a woman's purse, like a man's billfold, were attached to her person. It might then amount to a kind of 'outer clothing,' which under the Court's cases would properly receive increased protection.") (internal citations omitted).

222. The current Fourth Amendment doctrine presents an oddity that the data coming from an effect (one's jacket or purse) is considered part of the person. This is partially because a study of effects has remained an undeveloped area of the law. Perhaps, this Article, and others that focus on effects, will give new purchase to the concept that effects can be analyzed separately from the other terms of art in the Fourth Amendment.

223. A physical touching would be a physical invasion under *Jones*, and reaching into clothing would violate an expectation of privacy under *Katz*. 132 S. Ct. at 948; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

information within the effect is protected from a search because it is considered part of the individual's person.

ii. Communication Signals of Effects

A more difficult question arises if police are able to intercept the signals coming from a bracelet, a shoe, or even a heart monitor without physically interfering with the person or device itself. If a sensor is relaying information constantly, and police can wirelessly collect that information, a real puzzle emerges about whether the police have conducted a search for Fourth Amendment purposes. No physical intrusion or trespass has occurred under the traditional understanding of trespass.[224] No court has addressed the expectation of privacy of information worn on the person, but obtainable by others. Further, unlike the home example, where the Supreme Court in *Kyllo* specifically prohibited police from collecting information emanating from the constitutionally privileged area of the home, here the person is in public and away from the home.[225]

Analyzing how courts might address this question under current Fourth Amendment law is a guessing game. On the one hand, the information revealed is quite private, sometimes involving health matters or personal life patterns.[226] This type of information (at least when aggregated) was recognized by the concurring Justices in *Jones* to warrant Fourth Amendment protection.[227] If a car being tracked to reveal personal information violates a reasonable expectation of privacy, so should a heart monitor revealing an elevated heartbeat at certain moments of the day.[228] Of course, the strength or weakness of a reasonable expectation of privacy claim necessarily depends on the type of data being revealed. If data from a Fitbit monitor only reveals the number of steps taken by its owner, and not the location of those steps, a claim that the owner had a reasonable expectation of privacy would be harder to sustain. Or if the information were deidentified such that the data were not linked to a particular person, such information would not have the same claims to privacy.[229] Importantly, *Jones* did not reach the question of whether short-term,

224. *See supra* notes 158–60 (discussing *Jones*).

225. *See supra* notes 214–17.

226. *See supra* note 75.

227. 132 S. Ct. at 956 (Sotomayor, J., concurring); Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 403 (2013) ("This anti-aggregation norm figured prominently into the Supreme Court's rejection of long-term, warrantless GPS surveillance in *United States v. Jones*.").

228. Peppet, *supra* note 32, at 93 ("[A] fitness monitor's separate measurements of heart rate and respiration can in combination reveal not only a user's exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures.").

229. *See* Schwartz & Solove, *supra* note 82, at 1847 ("In sum, whether information can be re-identified depends on technology and corporate practices that permit the linking of de-identified data with already-identified data. Moreover, as additional pieces of identified data become available, it becomes easier to link them to de-identified data because there are likely to be more data elements in

nonaggregated tracking violated a reasonable expectation of privacy, which might occur with certain IoT surveillance.

iii. Networked Information of Effects

The third-party doctrine resolves the Fourth Amendment question whether police can access the same personal information directly from the third-party provider. The answer is generally yes.[230] If individuals give up personal information to third parties in return for better insights about health, fitness, or the like, then the third-party doctrine does not protect that information from police requests.[231] Obviously, the choice is up to the third party whether to comply with police investigations without a warrant. However, individuals will have no independent Fourth Amendment protection if the existing third-party doctrine controls. This lack of protection exists even if the private third party has a privacy policy ostensibly protective of consumers. As will be discussed in Part III, this failure of the *Katz* reasonable expectation of privacy test supports the argument for a new theory based on digital curtilage.

c. Investigating Effects Located in Cars

Police investigators regularly monitor the travel patterns of suspected criminals.[232] As *Jones* demonstrates, placing a GPS tracking device on an automobile can be an effective mechanism to establish a suspicious connection

---

common."); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 36 (2011) (finding that risks to privacy arising from reidentification of deidentified data is overstated); *cf.* Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 34 (2010); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1746 (2010) ("Once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success.").

230. Fourth Amendment scholars such as Professor Stephen Henderson have distinguished a broad third-party doctrine from "a limited third party doctrine" which holds that information is protected if it is transmitted for that third party's use. Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 524, 528 (2005).

231. Mearian, *supra* note 217 ("Rainey Reitman, activism director for privacy advocacy group Electronic Frontier Foundation, said wearable device companies that collect data from users in cloud services can be subpoenaed -- just as Google and Microsoft have been for years. . . . There is a clause in the privacy policies of most service providers that states they will release data in response to valid legal requests, Reitman said.").

232. At the time the *Jones* case was decided, the FBI admitted that it had over 3,000 active GPS tracking devices in use; state and local police would obviously add to that number. Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J.: DIGITS (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling [http://perma.cc/4QMQ-WZSW]; Pete Yost, *FBI Chief Describes GPS Problem from Court Ruling*, SAN DIEGO UNION-TRIB. (Mar. 7, 2012, 11:55 AM), http://www.utsandiego.com/news/2012/mar/07/fbi-chief-describes-gps-problem-from-court-ruling [http://perma.cc/9S9N-GKS7].

with a place or a pattern of criminal activity.[233] Under the Fourth Amendment, the car is itself an effect—with or without IoT capabilities.[234] As with the "effects in homes" analysis, a traditional Fourth Amendment analysis provides some guidance on how to analyze the definition of a search but does not answer all of the questions.

i. Physical Object & Digital Data of Effects in Cars

Automobiles have a particular, but not primary, place among Fourth Amendment protections.[235] The Supreme Court has recognized a reasonable expectation of privacy, but one tempered by the exigencies of an object that is mobile, heavily regulated, and often in public space.[236] The automobile exception allows stops and searches of automobiles under a host of circumstances.[237] At the same time, physical intrusions, including minor physical interference, can rise to a Fourth Amendment violation under a trespass theory.[238]

For police officers seeking the IoT information inside a car—location, travel patterns, speed, etc. located in the car's "black box"—searching the physical object of the car and recovering the digital data might be difficult without a warrant. Under a physical intrusion analysis, such a physical inspection of the car and extraction of recorded data would be a search more invasive than merely affixing a GPS device to the bottom of the car and recovering the data from the device.

---

233. *See* United States v. Jones, 132 S. Ct. 945 (2012).

234. *Id.* at 949 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment.").

235. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 566 (1991); Wyoming v. Houghton, 526 U.S. 295, 309 (1999) (Stevens, J., dissenting); California v. Carney, 471 U.S. 386, 389–90 (1985); United States v. Ross, 456 U.S. 798, 809 (1982); Cardwell v. Lewis, 417 U.S. 583, 597 (1974); Chambers v. Maroney, 399 U.S. 42, 61–62 (1970); Brinegar v. United States, 338 U.S. 160 (1949); Carroll v. United States, 267 U.S. 132 (1925). *See generally* Daniel T. Gillespie, *Bright-Line Rules: Development of the Law of Search and Seizure During Traffic Stops*, 31 LOY. U. CHI. L.J. 1, 2 (1999).

236. South Dakota v. Opperman, 428 U.S. 364, 367 (1976) ("Although automobiles are 'effects' and thus within the reach of the Fourth Amendment warrantless examinations of automobiles have been upheld in circumstances in which a search of a home or office would not. The reason for this well-settled distinction is twofold. First, the inherent mobility of automobiles creates circumstances of such exigency that, as a practical necessity, rigorous enforcement of the warrant requirement is impossible. But the Court has also upheld warrantless searches where no immediate danger was presented that the car would be removed from the jurisdiction. Besides the element of mobility, less rigorous warrant requirements govern because the expectation of privacy with respect to one's automobile is significantly less than that relating to one's home or office.") (internal citations omitted).

237. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405 (2005) (speeding and then dog sniff of marijuana); Maryland v. Pringle, 540 U.S. 366 (2003) (speeding); Atwater v. City of Lago Vista, 532 U.S. 318, 322 (2001) (seatbelt infraction); Whren v. United States, 517 U.S. 806 (1996) (civil traffic infraction).

238. *See Jones*, 132 S. Ct. at 949 (holding that placement of the GPS device without any other intrusion was a search).

The ordinary automobile exception would not, at first blush, cover a search of the computer data or electronic components inside a car's black box computer.[239] Under a reasonable expectation of privacy analysis, citizens might expect that police could observe their cars. But they do not expect their cars to be dismantled to obtain revealing information.[240] That said, the expectation of privacy concerning a car's black box is contestable under the same justifications of mobility and regulation that support the broader automobile exception.[241] Further, if a police stop were based on a traffic infraction or a traffic accident, an argument could be made that the internal car data could be evidence of the crime.[242] Whether this data could be obtained directly without a warrant is an open question, although other avenues to access the information exist.[243]

ii. Communication Signals of Effects in Cars

Communication signals from an IoT device in the car presents a difficult Fourth Amendment question. Using our hypothetical example, if the police developed technology to intercept the equivalent of OnStar transmissions from the IoT device in the suspect's car before it reached the OnStar central command, there would be a question whether this action was a search for Fourth Amendment purposes.

Under a physical intrusion-trespass analysis, such conduct could not constitute a search because the interception of data occurred without physical intrusion into the effect. Again, parallel to the home situation, without a physical intrusion there is no trespass, and thus no search, under *Jones*.[244]

Under a reasonable expectation of privacy analysis, however, the answer remains unclear. Unlike the home which the Supreme Court has been willing to

239. In *Knowles v. Iowa*, the Supreme Court disallowed searches incident to traffic offenses. 525 U.S. 113, 118 (1998). In *Arizona v. Gant*, the Court disallowed searches incident to arrest unless "it is reasonable to believe the vehicle contains evidence of the offense of arrest." 556 U.S. 332, 351 (2009). An ordinary stop of a car would not necessarily allow for a full search of a car's engine and data.

240. *But see* United States v. Flores-Montano, 541 U.S. 149, 151 (2004) (allowing for the dismantling and searching of a car at the international border).

241. Pennsylvania v. Labron, 518 U.S. 938, 940 (1996) ("Our first cases establishing the automobile exception to the Fourth Amendment's warrant requirement were based on the automobile's 'ready mobility,' an exigency sufficient to excuse failure to obtain a search warrant once probable cause to conduct the search is clear.").

242. People v. Christmann, 776 N.Y.S.2d 437, 439, 441–42 (Just. Ct. 2004) (allowing for search of electronic data after a car accident); *see id.* ("[T]he immediate download of information from the Defendant's SDM is permitted and required by [state statute] and is not violative of the Defendant's rights to be free from unreasonable searches pursuant to the United States or New York Constitution.").

243. For example, if the car had been impounded or otherwise taken into police custody, such searches might be condoned under the inventory exception. *See* South Dakota v. Opperman, 428 U.S. 364, 376 (1976) (allowing for inventory searches).

244. *See supra* notes 158–60.

privilege as protected, automobiles are not similarly situated. Even home-like automobiles (mobile homes, etc.) are considered to lack the same reasonable expectation of privacy given to homes.[245] Courts have routinely held that cars in public areas should be provided little expectation of privacy.[246] From radar guns, to fly-over speed traps, to tollbooth tracking, speed and location have rarely been protected. Automated license plate readers regularly provide geolocational data about cars and travel patterns.[247] Thus, at least under a traditional analysis, communication signals from IoT devices about the public location of the car would not be able to claim a reasonable expectation of privacy. With a diminished expectation of privacy, courts would find no Fourth Amendment search.[248]

Further, any protection may depend on the form of the signals. OnStar communicates in much the same way as a cellphone.[249] Generally, a person making a cellular call from a phone would maintain Fourth Amendment protection in the content of the call. Logically, that protection should extend to a car calling on a person's behalf. But other information—who called, when, for how long, from where—may not fit this content-based cellular phone parallel. Under *Smith v. Maryland* these other facts may be unprotected because noncontent data shared with third parties has been deemed to fall outside of Fourth Amendment protection.[250] These data trails remain an open question for Fourth Amendment analysis.

245. California v. Carney, 471 U.S. 386, 390–394 (1985) (tracing the history and justifications of the exception and concluding that a mobile home fell under the automobile exception because of its potential mobility).

246. United States v. Chadwick, 433 U.S. 1, 12–13 (1977) ("One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. . . . It travels public thoroughfares where both its occupants and its contents are in plain view.") (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974)); New York v. Class, 475 U.S. 106, 113 (1986) ("Every operator of a motor vehicle must expect that the State, in enforcing its regulations, will intrude to some extent upon that operator's privacy."); *Opperman*, 428 U.S. at 368 ("Automobiles, unlike homes, are subjected to pervasive and continuing governmental regulation and controls, including periodic inspection and licensing requirements.").

247. Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 403 (2014).

248. The one caveat to this is Justice Alito's concern in *Jones* that aggregation of this information might run afoul of the Fourth Amendment. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience.").

249. Jeremy Laukkonen, *GM's OnStar Service: How Does It Work?*, ABOUT AUTOS (Dec. 11, 2014), http://cartech.about.com/od/Safety/a/Gms-Onstar-Service-How-Does-It-Work.htm [https://perma.cc/A6ZU-URNJ].

250. *See generally* 442 U.S. 735 (1979).

iii. Networked Information of Effects in Cars

Police interested in obtaining information about the car straight from the IoT service provider would have a much easier time because of the third-party doctrine. Consumers regularly sign away personal information in contractual agreements that few people read.[251] Car companies, insurance companies, and monitoring companies routinely mine this data to improve service of the vehicle, but the same information is available to law enforcement.[252] Again, with the third-party doctrine in effect, an individual would have little recourse under the Fourth Amendment to challenge a request by police to obtain data being tracked and recorded by the monitoring company.

d. Investigating Digital Effects—Smartphones

Smartphones can be considered a physical object, a digital storage archive, or a connection to the larger world of the Internet of Things.[253] Some commentators believe that the smartphone—or its progeny[254]—will be the key connector between individuals and the Internet of Everything.[255] As discussed, the Supreme Court acknowledged smartphones to be a different type of digital effect, requiring a different type of analysis.[256] For law enforcement, cellphones as minicomputers offer a wealth of investigative leads.[257] As was

---

251. *Jones*, 132 S. Ct. at 963 (Sotomayor, J., concurring) ("Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen."); *see also* Thomas Garry et al., *Intelligent Transportation Systems: Personal Data Needs and Privacy Law*, 39 TRANSP. L.J. 97, 112, 125 (2012). *See generally* Jennifer Valentino-DeVries, *OnStar Set to Start Tracking, Sharing More Data from Cars*, WALL ST. J.: DIGITS (Sept. 21, 2011, 8:54 AM), http://blogs.wsj.com/digits/2011/09/21/onstar-set-to-start-tracking-sharing-more-data-from-cars [https://perma.cc/B5RC-M4QC].

252. Cecilia Kang & Michael Fletcher, *As Automakers Tap Smartphone Technology, Concerns Grow About Use of Drivers' Data*, WASH. POST (Jan. 9, 2014) https://www.washingtonpost.com /business/economy/as-automakers-tap-smartphone-technology-concerns-grow-about-use-of-drivers-data/2014/01/09/91a505f2-78a0-11e3-b1c5-739e63e9c9a7_story.html [http://perma.cc/2VYY-3G7W] ("Police want black-box data from crashes if it can be helpful in criminal prosecutions, while insurance companies can use it to assess what happened at an accident as they settle claims. Also, lawyers sometimes review black-box data when trying to decide whether to take a case. As a general matter, law enforcement officials can access it through subpoenas or, in the case of insurance companies, through fine print in contract provisions that few consumers ever read.").

253. Riley v. California, 134 S. Ct. 2473, 2489 (2014) (discussing how smartphones are really "minicomputers").

254. As the Supreme Court pointed out in *Riley*, the smartphone technology at issue had not even been invented fifteen years before the case. *See id.* at 2484.

255. Tom Mighell, *The "Internet of Things" in Law Practice*, LAW PRAC., May–June 2014, at 28, 29 ("For most of us, the device that currently makes the Internet of Things most possible is the smartphone. Whether we like it or not, our phones collect a lot of data on us, primarily in relation to our location.").

256. *See supra* Part I.

257. Mason, *supra* note 86, at 1160 ("Smartphones regularly transmit the name, location, and signal strength of nearby networks to a company like Apple or Google, enabling the phone company to pinpoint a user's location. Additionally, many popular apps use and occasionally share location data absent the user's knowledge or consent.").

clear in the facts of *Riley*, incriminating evidence, unrelated to the arrest, can be stored on the suspect's phone and prove useful for law enforcement agents investigating crime.[258]

i. Physical Object & Digital Data in Smartphones

In deciding the narrow question of whether police needed a warrant to search a cellphone incident to arrest, the Supreme Court in *Riley* opined at length about the privacy interests in digital information stored on one's phone.[259] As discussed earlier, while *Riley* focuses on the search incident to arrest problem, the same analysis would also likely hold for searches of smartphones not incident to arrest.[260] Police would only be able to search the physical exterior of a phone if they had legal justification.[261] Any search of the digital content of the phone would be a search, and an unreasonable one without a warrant.

This conclusion can be supported under either a *Jones* or *Katz* and *Riley* rationale. Under *Jones*, scrolling through the smartphone would be a physical intrusion into the private property with the purpose of obtaining information. Under *Katz* and *Riley*, the privacy interests in the personal data are significant enough to require a warrant. Most closed containers—digital or not—are protected.[262] Applying this logic to a search of a smartphone, one would likely find that a physical search of data would violate the Fourth Amendment.

ii. Communication Signals of Smartphones

The *Riley* logic would likely influence analysis of the Fourth Amendment protection afforded to signals intercepted from a smartphone. Could the police intercept what they likely could not download physically or directly? Under existing law, such a virtual interception would not be a search under the physical intrusion-trespass rationale of *Jones*. Further, the Supreme Court has not resolved whether such interception of data would violate an expectation of privacy. Clearly, direct interception of communication content seems to run

258. Interestingly, the information in Wurie's cellphone was also protected, even though it was much less revealing. None of the qualitative or quantitative differences of digital data discussed in *Riley* existed in *Wurie*, and yet the Supreme Court required a warrant in both cases.

259. *Riley*, 134 S. Ct. at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

260. *See* United States v. Chadwick, 433 U.S. 1, 12 (1977); *supra* Part II.B.2.

261. Touching the object would be a physical intrusion or trespass under *Jones*. Examining the outside (at least what could not be seen from plain view) would be a potential violation of an expectation of privacy. However, as most cellphone exteriors are completely unrevealing this might not matter much. *Riley*, 134 S. Ct. at 2485 ("Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case.").

262. *Chadwick*, 433 U.S. 1 (1977) (footlocker).

afoul of privacy interests dating back to Charles Katz's original conversation in the phone booth.[263] However, some (noncontent) data might not be protected (including short-term locational data).[264] The point is that courts have not yet resolved what parts of our smartphone communication and data should be protected under a reasonable expectation of privacy. Even *Riley*, a case that acknowledged the importance and complexity of smartphone data, offered no answers to the question whether data communicating with the cloud deserved Fourth Amendment protection.[265]

iii. Networked Information of Effects

The third-party doctrine has been well analyzed when it comes to cellphone companies, Internet search engines, and social media providers.[266] Currently, the Constitution provides little protection for information citizens voluntarily provided to third-party communication companies.[267] While privacy policies and other consumer protections may exist, the Fourth Amendment leaves citizens unprotected.

e. Investigating Pure Effects

The Internet of Things began demonstrating its value in the industrial space, as manufacturing processes tracked items in granular detail. This ability to track and monitor items through the use of IoT sensors could prove useful to police investigating the illegal drug trade. Through RFID technology, a package might reveal origin and route of travel.[268] Police interested in investigating a package mailed to our suspected drug dealer would welcome technology to track packages that potentially contain illegal narcotics, drug paraphernalia, laundered money, or the like.[269] Pattern-matching technologies might reveal a drop location for drugs or a link between different suspected drug addresses.

---

263. *See supra* note 156 and accompanying text. This privacy concern also spurred the creation of the Wiretap Act.

264. This type of information is the type of data at issue in the Stingray interception cases. Hosein & Palow, *supra* note 82, at 1085–86 ("IMSI catchers and mobile interception devices make it possible for the government directly to monitor mobile communications without having to involve the carriers."); Pell & Soghoian, *supra* note 100, at 144.

265. *Riley*, 134 S. Ct. at 2491 (discussing cloud computing).

266. *See generally* Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 879 (2014); Henderson, *supra* note 6, at 705–06.

267. *See supra* note 165 and accompanying text; Smith v. Maryland, 442 U.S. 735 (1979).

268. Yochai Benkler, *Open Wireless vs. Licensed Spectrum: Evidence from Market Adoption*, 26 HARV. J.L. & TECH. 69, 119 (2012) (discussing the technology behind FedEx and UPS package tracking).

269. *See, e.g.*, United States v. Lakoskey, 462 F.3d 965, 970 (8th Cir. 2006), *amended on reh'g* (Oct. 31, 2006); United States v. Mathis, 122 F. App'x 173, 174 (6th Cir. 2004); United States v. Mallory, 709 F. Supp. 2d 451 (E.D. Va. 2010) (discussing the federal prosecution of mail fraud built around tracking of a FedEx package).

For purposes of this analysis, imagine the police see our suspect standing next to a package. The package is not abandoned or physically held by the suspect.[270] The package is clearly in his possession, but it is also a standalone Fourth Amendment effect. The package is a plain old sealed box. The package also contains a communicating sensor of semiprivate information. The ambiguities revealed in analyzing this package can be extrapolated to all pure effects, including most items with RFID chips or other equivalent sensor devices, not found in a home, in a car, or on a person.

i. Physical Object

The Fourth Amendment protects personal property independent of whether the effect is found in a home or on a person, as long as it is in some way concealed.[271] As the Supreme Court wrote:

> For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.[272]

In other words, just as a police officer could not search a bag or a briefcase without a warrant, the police officer could not physically open and search the package.[273] The police action would both be considered a physical invasion of private property (a closed container) and violate a well-settled reasonable expectation of privacy.[274]

---

270. This clarification is necessary to establish an ownership interest or reasonable expectation of privacy (Fourth Amendment standing), and avoid the argument that the package was abandoned. *See* Rakas v. Illinois, 439 U.S. 128, 148 (1978); California v. Greenwood, 486 U.S. 35 (1988).

271. United States v. Karo, 468 U.S. 705, 730–31 (1984) ("The Court has developed a relatively straightforward test for determining what expectations of privacy are protected by the Fourth Amendment with respect to the possession of personal property. If personal property is in the plain view of the public, the possession of the property is in no sense 'private' and hence is unprotected: 'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.' When a person's property is concealed from public view, however then the fact of his possession is private, and the subject of Fourth Amendment protection.") (internal citation omitted).

272. United States v. Ross, 456 U.S. 798, 822 (1982).

273. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 598 (1991) (Stevens, J., dissenting) ("Every citizen clearly has an interest in the privacy of the contents of his or her luggage, briefcase, handbag or any other container that conceals private papers and effects from public scrutiny. That privacy interest has been recognized repeatedly in cases spanning more than a century."); United States v. Chadwick, 433 U.S. 1 (1977) (footlocker).

274. *Chadwick*, 433 U.S. at 12; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

ii. Digital Data and Communication Signals

The more interesting question would be whether the officer could examine the outside of the box for the information—digital, coded, or sensor-driven information coded within—to track the past history of the box. The plain view exception would provide some justification for access, if the information were plainly evident without manipulation.[275] As long as the police officers were lawfully present, with lawful access, and could plainly view immediately incriminating evidence, such a search would not violate the Fourth Amendment.[276] However, as may be obvious, bar codes or quick response codes (QR codes)[277] are rarely immediately incriminating, even if some rather simple technology could likely read the barcodes without manipulation.[278] If there was need to physically touch the package to obtain the data, such a physical invasion might constitute a trespass, as in *Jones*.[279] If not, collecting the embedded data would likely not violate an expectation of privacy, because the information—the code—was available for all to see.

At a second level of inquiry, the question would be whether any sensor data emanating from the package could be intercepted. For example, if the police officer could intercept the information without touching the package, such an action would not involve a trespass-physical invasion and would not violate any established expectation of privacy.[280] Most mail delivery systems have sensors that provide sensor data with a swipe of a bar code reader.[281] Some systems communicate the package's location with more sophisticated tracking technology. In fact, major shipping companies provide the possibility of tracking the package on the Internet if one is in possession of the tracking number.[282] While the contents of the package might be protected by an

275. *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366 (1993); Arizona v. Hicks, 480 U.S. 321 (1987); Coolidge v. New Hampshire, 402 U.S. 443 (1971).

276. *Dickerson*, 508 U.S. at 375 ("The rationale of the plain-view doctrine is that if contraband is left in open view and is observed by a police officer from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy and thus no 'search' within the meaning of the Fourth Amendment—or at least no search independent of the initial intrusion that gave the officers their vantage point.").

277. QR codes are the black and white, matrix like box used as barcodes for smartphone applications.

278. *See generally* Jerry Brito, *Relax Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature*, 2004 UCLA J.L. & TECH. 5 (discussing RFID technology); Manoj Govindaiah, *Driver Licensing Under the Real ID Act: Can Current Technology Balance Security and Privacy?*, 2006 U. ILL. J.L. TECH. & POL'Y 201, 211 (discussing encryption differences between barcodes and RFID).

279. Or a seizure as in *Hicks*. 480 U.S. at 327.

280. Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 239, 264 (1994).

281. *Customer Support Center*, FEDEX, http://www.fedex.com/us/customersupport/tracking (last visited Mar. 28, 2016).

282. M. Sean Fosmire, *Intranets and Extranets—The Extension of Web Technology to the Distribution of Private Information*, 77 MICH. B.J. 412, 414 (1998) ("The most widely known

expectation of privacy, the shipping data—including the contents, the sender, the intended receiver, and other information not plainly visible—would likely not be protected.[283] While the data could be quite private, it is also communicating to the outside world. Depending on the definition of the effect, this information is either part of the effect or separate from the effect. This definitional challenge is the subject of Part III.

iii. Networked Data

Finally, similar to the previous analysis, if the police sought the same information directly from the third-party package delivery service, there would be no Fourth Amendment issue under the third-party doctrine. In fact, the U.S. Postal Service and most private carriers, like FedEx and UPS, scan, record, and carefully monitor all mail and packages delivered.[284]

2. Gaps in the Fourth Amendment Doctrine

Five major insights can be gained from the foregoing analysis. First, Fourth Amendment doctrine remains unsettled as applied to the Internet of Things. Many commentators have bemoaned the confused state of Fourth Amendment doctrine in general,[285] and the complications arising from the Internet of Things only adds to the muddled landscape. Second, the physical intrusion-trespass analysis from *Jones* leaves many IoT effects unprotected from virtual inspection or interception of communications data. If understood merely as a physical intrusion, the protection adds little in a world of digital tracking and data trails. Third, although the reasonable expectation of privacy test is generally sympathetic to the privacy interests in digital information, its

example of an extranet is FedEx's web site, which provides its customers with a web-based database for tracking the packages that are *en route* within FedEx's system.").

283. The analogy would be to *Smith v. Maryland*, 442 U.S. 735 (1979), although the large-scale mass surveillance collection might make it more analogous to a mass meta-data collection program.

284. Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html [https://perma.cc/M28Z-G4XA] (detailing the "Mail Isolation Control and Tracking program, in which Postal Service computers photograph the exterior of every piece of paper mail that is processed in the United States—about 160 billion pieces last year").

285. *See, e.g.*, Morgan Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 555 (1996) ("Fourth Amendment theory is in tatters at the end of the twentieth century. The disarray in the Supreme Court's recent case law has been explored in numerous scholarly articles and judicial dissents."); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011) ("Scholars complain that the law is 'a mess,' 'an embarrassment,' and 'a mass of contradictions.'") (quoting Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149 (1998)); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence.").

protections are weak and police can easily circumvent it using the third-party doctrine.

In addition, two major gaps remain: How should courts treat the stored data in the smart object? And, how should courts treat the communication signals emanating from the object? While the Supreme Court has not definitively ruled on the subject, a reasonable prediction is that some stored data (like data in a computer) likely would be protected under a reasonable expectation of privacy test. There is little consensus, however, about how to evaluate the sensor signals emanating from the device. The unresolved issues invite the question of whether the Internet of Things requires a reevaluation of the Fourth Amendment understanding of "effects." If the definition of an effect were to include internal data *and communication signals*, then this redefinition could neatly fill the doctrinal gaps currently in existence. This redefinition project is the subject of the next Part.

III.
AN ARGUMENT FOR REDEFINING EFFECTS IN AN IOT WORLD

Under existing Fourth Amendment doctrine, a gap exists in how to analyze an effect in the Internet of Things. If an effect is defined merely as the "dumb" physical object, then the "smart" sensor information emanating from the object and the digital information inside may not be protected. If an effect is defined as the physical object, plus the digital information located in the device and the communication signals to a third-party network, then a whole new Fourth Amendment threshold has been created without clear boundaries.

This Part reexamines the fundamental question of definition. First, this Part addresses whether the Fourth Amendment's text can be read to expand "effects" to a modern understanding beyond mere physical objects. By examining other terms of art in the Fourth Amendment, this Part concludes that such an expansion parallels other interpretations of the Fourth Amendment. Second, this Part looks to see if such an expanded definition is consistent with Fourth Amendment theory, looking at foundational principles informed by privacy-security interests, property interests, and core constitutional interests. The next Part, then, develops the framework of what a Fourth Amendment effect connected to the Internet of Things might look like. Building off a theory of "personal curtilage" developed in an earlier article on personal privacy in a high-tech surveillance world,[286] Part IV develops the theory of "digital curtilage"[287] to mark off the boundaries of a communicating

286. Ferguson, *supra* note 27, at 1288 ("The theory of personal curtilage turns on persons being able to control the constitutionally protected areas of their lives in public by signifying that they intend for an area to be secure from physical and sense-enhancing invasion.").

287. Joseph A. Giordano, *Clouded Computing: The Foggy Application of the Fourth Amendment in Technology*, 39 RUTGERS COMPUTER & TECH. L.J. 141, 184 (2013) (using the term "digital curtilage" but defining it differently than in this Article).

effect.[288] The goal is to fill the doctrinal gap by demonstrating that a definition of effects can include both the digital information in the device as well as some of the communicating signals coming from the device.

A. Textual Grounding

As an initial matter, it is worth exploring whether the constitutional text can bear the weight of new meanings. A pure originalist would have an easy time dismissing any expansion of the term "effects" to include anything other than the effects existing at the time of the Framers.[289] But the Supreme Court has not fully adhered to pure originalism, and even conservative justices have been willing to expand constitutional protections to address modern technologies.[290] In fact, a close reading of Fourth Amendment case law demonstrates that each of the chosen terms of art—persons, houses, papers, and effects—have been given a more expansive reading than the pretechnological and preindustrial world of the Founders. While this textual expansion has largely developed under a reasonable expectation of privacy analysis, the constitutional understanding of what areas are constitutionally protected has unquestionably grown to reflect changes in society and technology.

1. Persons

The Fourth Amendment protects "persons," which of course includes the physical body understood to be a human being at the time of the founding.[291] "Persons," thus, includes intrusions into the human body to draw blood[292] or obtain saliva,[293] but has also been extended to cover excretions from the human

288. Digital curtilage is defined and discussed *infra* Part IV. Digital Curtilage: Redefining Effects in the Internet of Things.

289. *See generally* Randy E. Barnett, *Trumping Precedent with Original Meaning: Not as Radical as It Sounds*, 22 CONST. COMMENT. 257, 257–59 (2005); Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849, 863–64 (1989).

290. For example, Justice Scalia recognized in *Kyllo*, "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." Kyllo v. United States, 533 U.S. 27, 36 (2001).

291. Joshua S. Levy, Note, *Towards A Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 499, 515 (2011) ("The text of the Fourth Amendment explicitly refers to both 'houses' and 'persons,' and searches involving homes and bodies are mainstays of criminal investigations and have been for years.").

292. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616 (1989) ("In light of our society's concern for the security of one's person, it is obvious that this physical intrusion, penetrating beneath the skin, infringes an expectation of privacy that society is prepared to recognize as reasonable.") (internal citations omitted); Schmerber v. California, 384 U.S. 757 (1966).

293. D. H. Kaye, *Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees*, 34 J.L. MED. & ETHICS 188, 191 (2006) ("Under a line of cases involving blood sampling, breathalyzers, urine specimens, and nail scrapings, the Court could rely on the dignitary interests related to physical invasions to find that buccal swabbing or saliva sampling for DNA analysis is a bona fide Fourth Amendment event."); *see also, e.g.*, Kohler v. Englade, 470 F.3d 1104 (5th Cir. 2006); Padgett v. Donald, 401 F.3d 1273 (11th Cir. 2005); Commonwealth v. Draheim, 849 N.E.2d 823 (Mass. 2006); State v. Martinez, 78 P.3d 769 (Kan. 2003).

body, such as urine[294] and breath in a breathalyzer.[295] DNA recovered from a person was obviously not considered by the Founders, but has been granted limited protection by the courts.[296] A search of "persons" has also been expanded to mean a search of clothing (pockets, etc.) as well as personal belongings. If a person carries a purse or bag, then such items are usually analytically subsumed as a search of the person and not a search of their effects.[297] Most expansively, corporations—formal entities without any human form—have been covered in the textual meaning of persons.[298] A Fourth Amendment "person" now also includes corporate persons.[299] This expansion is not rewriting the text, but merely broadening the modern definition of "persons" to match the needs of an advancing society.

2. Houses

The Fourth Amendment's text protects "houses," which originally meant the homestead, but has also been expanded beyond the four walls of a traditional house.[300] The concept of curtilage has extended the core protection

294. *Accord* Ferguson v. City of Charleston, 532 U.S. 67 (2001); Chandler v. Miller, 520 U.S. 305 (1997); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989); *Skinner*, 489 U.S. at 617 ("Unlike the blood-testing procedure at issue in *Schmerber*, the procedures prescribed by the FRA regulations for collecting and testing urine samples do not entail a surgical intrusion into the body. It is not disputed, however, that chemical analysis of urine, like that of blood, can reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic. Nor can it be disputed that the process of collecting the sample to be tested, which may in some cases involve visual or aural monitoring of the act of urination, itself implicates privacy interests.").

295. *Skinner*, 489 U.S at 616–17 ("Subjecting a person to a breathalyzer test, which generally requires the production of alveolar or 'deep lung' breath for chemical analysis, implicates similar concerns about bodily integrity and, like the blood-alcohol test we considered in *Schmerber*, should also be deemed a search.") (internal citation omitted).

296. Maryland v. King, 133 S. Ct. 1958, 1968–69 (2013) ("It can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search. Virtually any 'intrusion into the human body' will work an invasion of 'cherished personal security' that is subject to constitutional scrutiny."); *see also, e.g.*, Nicholas v. Goord, 430 F.3d 652 (2d Cir. 2005); United States v. Sczubelek, 402 F.3d 175 (3d Cir. 2005); United States v. Kincade, 379 F.3d 813 (9th Cir. 2004); Tracey Maclin, *Government Analysis of Shed DNA Is a Search Under the Fourth Amendment*, 48 TEX. TECH L. REV. 287 (2015).

297. *See supra* notes 221–22 (discussing purses and other bags carried on one's person). This analysis may be a bit inexact, as one can always differentiate, for example, a pants pocket and a person wearing the pants. But courts tend not to do a separate analysis due to the close proximity of pockets to one's person.

298. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920).

299. Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*, 41 HASTINGS L.J. 577, 644 (1990) (recognizing that "the Court granted fourth amendment rights to corporations to protect what is arguably a form of property: corporate papers") (citing Hale v. Henkel, 201 U.S. 43 (1906)); *see also* Dow Chem. Co. v. United States, 476 U.S. 227 (1986); *Silverthorne Lumber*, 251 U.S. at 385.

300. Quintana v. Commonwealth, 276 S.W.3d 753, 757 (Ky. 2008) ("The fact that the curtilage as well as the home itself is entitled to Fourth Amendment protection and an expectation of privacy is premised on strong concepts of intimacy, autonomy, and sanctuary that develop around home and family life, and the fact that many related activities will occur outside the house."); Carrie Leonetti,

of homes beyond the physical home.[301] Curtilage has been defined as "the area around the home to which the activity of home life extends."[302] While dependent on a four-factor test, the area exists and warrants protection of the Fourth Amendment as a constitutionally protected space.[303] As the Supreme Court stated in *Florida v. Jardines*, "We therefore regard the area 'immediately surrounding and associated with the home'—what our cases call the curtilage—as 'part of the home itself for Fourth Amendment purposes.'"[304]

Curtilage expanded beyond houses and is now understood to include barns,[305] sheds,[306] and other outbuildings.[307] But the protection of homes also reaches temporary homes, including apartments,[308] hotels,[309]

Open Fields in the Inner City: Application of the Curtilage Doctrine to Urban and Suburban Areas, 15 GEO. MASON U. C.R. L.J. 297, 298–303 (2005).

301. United States v. Dunn, 480 U.S. 294, 300 (1987) ("[T]he Fourth Amendment protects the curtilage of a house and that the extent of the curtilage is determined by factors that bear upon whether an individual reasonably may expect that the area in question should be treated as the home itself.") (citing Hester v. United States, 265 U.S. 57 (1924)).

302. Oliver v. United States, 466 U.S. 170, 182 n.12 (1984); United States v. Gorman, 104 F.3d 272, 274 (9th Cir. 1996) ("For the purposes of the Fourth Amendment, curtilage is important because it extends to a larger area the right to privacy a person enjoys inside the home: '[A]n individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.'").

303. *Dunn*, 480 U.S. at 300 ("[In *Oliver*] we recognized that the Fourth Amendment protects the curtilage of a house and that the extent of the curtilage is determined by factors that bear upon whether an individual reasonably may expect that the area in question should be treated as the home itself."); California v. Ciraolo, 476 U.S. 207, 212–13 (1986); Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 63 (2002) ("*United States v. Dunn* elevated *Oliver's* dicta on the meaning of curtilage to law.").

304. 133 S. Ct. 1409, 1414 (2013).

305. *Dunn*, 480 U.S. at 307–08 (Brennan, J., dissenting) ("State and federal courts have long recognized that a barn, like many other outbuildings, is 'a domestic building constituting an integral part of that group of structures making up the farm home.' Consequently, the general rule is that the '[c]urtilage includes all outbuildings used in connection with a residence, such as garages, sheds, [and] *barns* . . . connected with and in close vicinity of the residence.'") (citing state cases).

306. Brown v. Oklahoma City, 721 P.2d 1346, 1349 (Okla. Civ. App. 1986) ("[C]urtilage . . . includes, among other things, garages, sheds, barns and the like.").

307. State v. Fierge, 673 S.W.2d 855, 856 (Mo. Ct. App. 1984) ("[C]urtilage includes all out-buildings used in connection with the residence, such as garages, sheds, barns, yards, and lots connected with or in the close vicinity of the residence."); State v. Lee, 253 P. 533, 534 (Or. 1927) ("Premises other than dwellings have been held within the protection of the Fourth Amendment; for example a barn. As construed by the courts from the earliest to the latest times, the words 'dwelling' or 'dwelling-house' have been construed to include not only the main but all of the cluster of buildings convenient for the occupants of the premises, generally described as within the curtilage.").

308. Robertson v. State, 740 N.E.2d 574, 576 (Ind. Ct. App. 2000) ("Individuals who live in apartments often hang decorations on outside doors and place doormats on the ground outside the door. Further, individuals who have apartments that exit immediately outside often place and keep personal items on their steps or porches. Simply because one lives in an apartment does not mean that he or she does not at times occupy the space immediately outside of the apartment home. Thus, one who lives in an apartment also treats the area immediately outside his or her apartment home as his or her curtilage."); Espinoza v. State, 454 S.E.2d 765, 767 (Ga. 1995) ("Like residents in single-family homes, apartment residents have a reasonable expectation of privacy in the curtilage surrounding their apartment."); State v. Murray, 527 P.2d 1303, 1308 (Wash. 1974) (en banc).

309. Stoner v. California, 376 U.S. 483 (1964).

motels,[310] and other immovable premises.[311] "Houses," thus, has come to mean a whole host of home-like settings that protect personal space and private activities akin to the traditional home.

3. Papers

"Papers"—including personal diaries, letters, and writings—have always been protected by the Fourth Amendment.[312] In addition, commercial records, including business documents, have also been considered papers worthy of Fourth Amendment protection.[313] However, as the world has digitized, code has replaced handwriting and electronic data has replaced paper. While the Supreme Court has yet to directly address whether papers includes digital media, courts and commentators assume that the Fourth Amendment's protection of papers also includes the protection of writings stored in digital form (be they on computers, smartphones, or other digital storage devices).[314]

4. Conclusion as to Effects

As discussed earlier, an effect can include all sorts of personal items.[315] Personal effects have grown from simple, tangible objects, to communicating, even sentient things.[316] Parallel to other terms in the Fourth Amendment, this expansion has been necessary to adapt to a changing world. The question is whether the textual definition of an "effect" should adapt as well. The following Sections discuss this redefinition, which involves some contested value choices, but the conclusion that at least as a textual matter, the language of the Fourth Amendment can bear the weight of new meanings.

---

310. State v. Davis, 937 P.2d 1110, 1113 (Wash. Ct. App. 1997); Miller v. United States, 357 U.S. 301, 314 (1958).

311. Eulis Simien, Jr., *The Interrelationship of the Scope of the Fourth Amendment and Standing to Object to Unreasonable Searches*, 41 ARK. L. REV. 487, 554 (1988) ("[Houses] is not limited to actual places of residence but has been interpreted to mean places 'where people live, work, and play' . . . ."); *see id.* at 555 (arguing "'houses' to include other immovable premises").

312. Boyd v. United States, 116 U.S. 616 (1886); *see also* Dripps, *supra* note 146, at 73.

313. G.M. Leasing Corp. v. United States, 429 U.S. 352 (1977) (books and records of General Motors); Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920) (books and records).

314. United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (holding that email files are protected under the Fourth Amendment); United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (analogizing computer files with physical files); Harper, *supra* note 28, at 246 ("Courts should treat digital representations of information as constitutional papers or digital effects that the Fourth Amendment secures.").

315. *See supra* Part II.A.

316. Mark Jaffe, *IoT Won't Work Without Artificial Intelligence*, WIRED (Nov. 12, 2014), http://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence [https://perma.cc/9TR6-AL4C]; Peter McOwan & Louis McCallum, *When Fridges Attack: The New Ethics of the Internet of Things*, GUARDIAN (Sept. 8, 2014, 2:00 AM), http://www.theguardian.com/science/alexs-adventures-in-numberland/2014/sep/08/when-fridges-attack-the-new-ethics-of-the-internet-of-things [http://perma.cc/4X8Z-TJJV].

B. Theoretical Grounding

Building off of this textual analysis, the next question is whether an expanded definition of an "effect" is consistent with Fourth Amendment theory. This Section presents three overlapping arguments about why the internal data and external signals emanating from IoT devices should be considered part of the effect itself. While analytically divided into separate sections covering constitutional, property, and privacy-security interests, these familiar constitutional principles overlap in many ways.

1. Core Constitutional Interests

Central to the discussion of how the language of the Fourth Amendment grew to incorporate more expansive readings of persons, houses, and papers, is the understanding that each expansion protected a relevant core constitutional interest. Blood, urine, and DNA can be removed from a person, but they still implicate a person's biological identity and thus personhood.[317] Curtilage exists at a distance from the four walls of the home, but protects activities similar to those that take place in the home.[318] Digital papers, while not literally printed on paper, protect the core Fourth Amendment interest of preserving a person's creativity and ideas.[319]

So, too, with the data and signals that emanate from an IoT device. The signals from the IoT sensors are what enables the object to do what it is supposed to do. These smart objects are not mere things, but, by design, also communication devices. The essence of the effect here is the sensor relaying data to another sensor. While we are primed to think in old-fashioned physical terms of the things we can see, the modern reality is inverted. What is valuable about IoT devices is the inside sensor data, not the outside covering. A Fitbit might work just as well without the cheap plastic covering, but what should be shielded from discovery is the working sensor communicating with another sensor. In fact, it would be rather backward to elevate protection for the unrevealing physical covering over the underlying intimate digital information.

---

317. Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 752 (2007) ("Raw DNA samples have the power to divulge the very essence of personhood: a person's phenotypic characteristics, gender, age, health, and genealogy."); *see also* Maclin, *supra* note 296.

318. Quintana v. Commonwealth, 276 S.W.3d 753, 757 (Ky. 2008) ("The fact that the curtilage as well as the home itself is entitled to Fourth Amendment protection and an expectation of privacy is premised on strong concepts of intimacy, autonomy, and sanctuary that develop around home and family life, and the fact that many related activities will occur outside the house.") (citing Dow Chem. Co. v. United States, 749 F.2d 307 (6th Cir. 1984)).

319. United States v. Seljan, 547 F.3d 993, 1014–17 (9th Cir. 2008) (Kozinski, J., dissenting) (emphasis added) (citation omitted), *cert. denied*, 129 S. Ct. 1368 (2009) ("But the Founders were as concerned with invasions of the mind as with those of the body, the home or personal property—which is why they gave papers equal rank in the Fourth Amendment litany. . . . What makes papers special-and the reason they are listed alongside houses, persons and effects-is the ideas they embody, ideas that can only be seized by reading the words on the page.").

Thus, the appropriate analysis to determine whether the communications of an IoT device can be intercepted and seized is whether the sensor data and signals fall within the constitutional interest of a smart effect. Because the data and signals are the core of the "thing" itself, both should be considered part of the redefined Fourth Amendment effect.

The argument is not merely functional, but almost ontological. The "thing" that is a smart effect is a "data-radiating thing." What is core to the data-radiating thing is the data, not the covering. The evolution of Fourth Amendment terms has never been merely about use or appearance or physical boundaries,[320] but about what happens in and around the protected area. The protection of curtilage exists not because curtilage looks like a home, or is bounded by the walls of the home, but because it provides a space to act like a home. Even a cheap motel room can be granted home-like status, not because a cheap motel is the same as a homestead, but because it allows guests to feel a sense, albeit temporary, of home-like protection. A core constitutional interests theory recognizes that in naming homes, persons, papers, and effects, certain characteristics about those areas or things ought to be protected even when the data are separated from the literal thing.

2. Property Interests

As the Supreme Court stated in *Jones*, "The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous."[321] This property-based focus has a long lineage in Fourth Amendment history and theory.[322] While effects have usually been analyzed as tangible property, they need not be so limited: the Fourth Amendment protects both tangible and intangible property.[323]

320. Each of these definitional choices provides an equally acceptable justification for defining the thing, but is just not the chosen focus of this Article.

321. United States v. Jones, 132 S. Ct. 945, 949 (2012).

322. United States v. Place, 462 U.S. 696, 701 (1983) ("In the ordinary case, the Court has viewed a seizure of personal property as *per se* unreasonable within the meaning of the Fourth Amendment unless it is accomplished pursuant to a judicial warrant issued upon probable cause and particularly describing the items to be seized."); J. Amy Dillard, *Big Brother Is Watching: The Reality Show You Didn't Audition for*, 63 OKLA. L. REV. 461, 487 (2011) ("[John Adams asserted that t]he moment the idea is admitted into society that property is not as sacred as the law of God, and that there is not a force of law and public justice to protect it, anarchy and tyranny commence.") (quoting THE FEDERALIST NO. 54 (James Madison)).

323. *See* LeClair v. Hart, 800 F.2d 692 (7th Cir. 1986) ("Following *Berger*, it has been clear that the Fourth Amendment embraces more than just the forced physical removal of tangible objects. . . . Indeed, *Berger* stands for the proposition that the government may seize intangible items such as the information contained in the financial documents which the IRS agents copied."); Berger v. New York, 388 U.S. 41, 57 (1967); Katz v. United States, 389 U.S. 347, 353 (1967); United States

Underlying this protection is the sense that information and other intangible items have value. Today, entire industries are built around collecting and studying nothing but data.[324] Thus, it is not surprising that the value of a device that records and transmits personal data includes both the tangible and intangible parts of the device. Again, going back to our Fitbit example, the value of the device is not simply the plastic band, but the stored data inside that tells the owner about his or her level of physical activity.[325]

Property principles, thus, strengthen the argument of why the data and communication signals coming from smart effects should be considered as part of the effect itself. The data is the valuable part of the ownership interest in the effect.[326] If owned by the user of the smart device, the user should control this information.[327] At a minimum, the owner of a device should be able to exclude others from accessing this information.[328]

Of course, this property line of analysis raises some difficult questions about who else owns the data. Most data created by the Internet of Things is owned both by the individual producing it and the company contracted to collect it for certain reasons.[329] In some cases, the companies claim sole control of the data and the intellectual property manipulating the data.[330] This contractual arrangement is fraught with difficulties of data ownership, use, and resale, issues the resolution of which lies beyond the scope of this Article.[331]

---

v. Warshak, 631 F.3d 266 (6th Cir. 2010) (discussing email content); eBay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (discussing robot crawlers mining data on websites).

324. Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443, 447 (2008); Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html [https://perma.cc/EP3F-GQD8].

325. In fact, for the companies producing the devices, the data may actually be more valuable than the object itself as the data can be sold to other companies.

326. Dickman v. Comm'r, 465 U.S. 330, 336 (1984) ("'Property' is more than just the physical thing—the land, the bricks, the mortar—it is also the sum of all the rights and powers incident to ownership of the physical thing. It is the tangible and the intangible. Property is composed of constituent elements and of these elements the right to use the physical thing to the exclusion of others is the most essential and beneficial. Without this right all other elements would be of little value.").

327. *See* Peppet, *supra* note 32, at 145 (recognizing that "privacy policies for consumer sensor devices often do not mention ownership of sensor data. Of the twenty products [examined], only four discussed data ownership explicitly. Of those that did clarify ownership of sensor data, three indicated that the *manufacturer*, not the consumer, owned the sensor data in question").

328. Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."); Int'l News Serv. v. Associated Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) ("An essential element of individual property is the legal right to exclude others from enjoying it."); White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1, 19 (1908) (Holmes, J., concurring) ("The notion of property . . . consists in the right to exclude others from interference with the more or less free doing with it as one wills.").

329. Peppet, *supra* note 32, at 145.

330. *See* Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 865–67 (2015).

331. *Id.*

For Fourth Amendment purposes, however, coownership does not remove the ability to exclude. So at a minimum, the owner of the device has a claim to control the data and a right to exert a measure of control excluding the government from any attempt at direct collection.

3. Privacy and Security Interests

Since *Katz*, privacy has been at the core of Fourth Amendment analysis. As set forth in Part I, the Internet of Things potentially exposes a vast amount of previously private details through sensor data. Applying a privacy rationale to protect the internal data from IoT devices is relatively straightforward. From *Katz* to the concurring opinions in *Jones*, the Supreme Court has recognized that technologically enhanced surveillance can violate the Fourth Amendment.[332] *Riley* also supports this argument in terms of protecting digital information stored on devices transmitting to the cloud.[333] Privacy, however, has some limitations as an analytical guide. First, it is never clear ex ante what the Supreme Court will find to be a reasonable expectation of privacy. Second, the third-party doctrine provides a broad work-around for information shared with other people.[334] Finally, to say that interception of data or a wireless signal violates a reasonable expectation of privacy does not necessarily answer the separate question whether a Fourth Amendment effect should be redefined to include those data and signals.

To address these limitations, this Article focuses on the corollary framework of security. The Fourth Amendment speaks of the right to be "secure" rather than the right to "privacy," and thus security may be a more appropriate framework to achieve a parallel protection for effects.[335] In general, the right to be secure has included the right to exclude the government from private areas.[336] As Professor Thomas Clancy has written, "[T]he Framers lived in a time that equated security with the ability to exclude. It provide[d] an easily identified and applied rule designed to protect an individual's right to be safe as to his or her person, house, papers, and effects."[337] As Clancy and

332. Tomkovicz, *supra* note 27, at 438 ("Official exploitation of a scientific or technological device should be considered a Fourth Amendment search at least when the effect is to enhance, augment or supplement human sensory abilities or other capacities in ways that have made it possible for the authorities to gain access to any information that otherwise would have been, or is highly likely to have been, imperceptible or inaccessible or would only have been, or is highly likely only to have been, perceived or acquired by means that are governed by the Fourth Amendment.").

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

334. *See supra* note 165 and accompanying text.

335. Rubenfeld, *supra* note 10, at 104 ("The Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*."). *See generally* Clancy, *supra* note 10.

336. Clancy, *supra* note 133, at 1059 ("Adams and his contemporaries repeatedly used the concept of 'security' to describe the quality of the right protected as to each person's life, liberty, and property.").

337. Clancy, *supra* note 10, at 362 (examining the historical roots and meaning of the right to exclude); *see also* Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("Security of

others have observed, this right to exclude—based on considerations of security—may offer a more robust protection than the right to privacy (especially in an age of high-tech surveillance).[338]

The right to exclude embraces both a preservation of personal autonomy and a protection against arbitrary or unreasonable intrusions.[339] Whether conceived of as the right to be left alone,[340] or a space for intimate activities,[341] or other protections of personal autonomy,[342] the Fourth Amendment has been read to encourage human development free from governmental surveillance. From general warrants[343] to mass surveillance[344] to high-tech snooping,[345]

---

the home must be guarded by the law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems."); United States v. Mendenhall, 446 U.S. 544, 550 (1980) (discussing the "constitutional right of personal security").

338. Clancy, *supra* note 133, at 1059 ("*Certain qualities in those objects valued: the right to be secure*. Adams and his contemporaries repeatedly used the concept of 'security' to describe the quality of the right protected as to each person's life, liberty, and property.") (emphasis added); Nowlin, *supra* note 25, at 1052 ("The word 'secure' in the text is closely associated with the phrase 'persons, houses, papers, and effects.' The guarantee of 'security' is extended to four enumerated interests: 'the right of the people to be secure in their persons, houses, papers, and effects.'"); Tomkovicz, *supra* note 27, at 341 ("The core value is, in essence, an interest in secrecy—in not having the details of our lives learned or exposed against our wishes. The Framers prized this aspect of 'the right to be let alone' as an essential foundation of a free society, and gave it a central place among the basic liberties enshrined in the Bill of Rights.").

339. Dow Chem. Co. v. United States, 476 U.S. 227, 240 (1986) (Powell, J., concurring in part and dissenting in part) ("The Fourth Amendment protects private citizens from arbitrary surveillance by their Government."); Boyd v. United States, 116 U.S. 616, 625 (1886) ("The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in their discretion, to search suspected places for smuggled goods, which James Otis pronounced 'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book;' since they placed 'the liberty of every man in the hands of every petty officer.'").

340. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

341. Kyllo v. United States, 533 U.S. 27, 37 (2001) (discussing the Fourth Amendment's protections of the intimate details of the home); California v. Ciraolo, 476 U.S. 207, 212–13 (1986) ("The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened."). *But see* Florida v. Riley, 488 U.S. 445, 463 (1989) (Brennan, J., dissenting) ("What, one wonders, is meant by 'intimate details'? If the police had observed Riley embracing his wife in the backyard greenhouse, would we then say that his reasonable expectation of privacy had been infringed? Where in the Fourth Amendment or in our cases is there any warrant for imposing a requirement that the activity observed must be 'intimate' in order to be protected by the Constitution?").

342. Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 152 (2002).

343. Clancy, *supra* note 133, at 1045 (noting Madison spoke of the "security against general warrants"); *Letter from James Madison to George Eve, Jan. 2, 1789*, *in* 5 WRITINGS OF JAMES MADISON 319 (Gaillard Hunt ed., 1900).

344. Rushin, *supra* note 66, at 288.

345. Tomkovicz, *supra* note 27, at 433 ("It is not implausible to contend that when the authorities use technology to access publicly-situated and physically-exposed details that otherwise would not or might not be perceptible to human faculties they violate privacy. If the exploitation of a device enables the government to learn details that could not or would not have been learned at all by

courts and commentators have been clear that protection from generalized, arbitrary searches runs to the core of the Fourth Amendment.[346]

In the context of the Internet of Things, the right to be secure offers a compelling justification about why the data and signals should be protected against governmental intrusion. The data at issue is largely private, encompassing sensitive home, personal, travel, and health information among other things.[347] The data trails reveal private patterns and information.[348] Even individualized data points—a single device monitored over time—invades a sense of personal autonomy.[349] Be it information about a pill bottle, a car's location, or a smartphone, there should be some ability to exclude the government from obtaining the information. Clearly, not all IoT devices will reveal intimate or personal details, but much of the details will nonetheless be information we would prefer to exclude from government monitoring.

Finally, an individual right to be secure is augmented by a collective right to be secure.[350] The fear of large-scale collection of personal information (real or virtual) without any judicial oversight also requires expanding the Fourth Amendment to protect data and communication signals in effects. If the data and signals from the IoT were routinely collected without any Fourth Amendment consideration, government officials could undertake a massive surveillance project without any constitutional check.[351] Billions of sensors could be monitored, implicating the lives of most Americans. Our data would be vulnerable to government collection and potential use with significant costs to individual freedom. Even the possibility of collection would shift the balance of power between citizens and the government.[352] Thus, constitutional

---

means known to the Framers, not even by methods subject to constitutional regulation, categorical rejection of a privacy claim based on 'public location' does not seem sensible.").

346. Ohm, *supra* note 19, at 89 ("Seizure of intangible property also implicates *security* interests, meaning the Fourth Amendment's promise that we will be secure from government coercion and unreasonable exercises of power.").

347. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1133 (2015).

348. *See* Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 187 (2012); Kerr, *supra* note 95, at 313–14.

349. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2015), http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/BF55-EUL5] ("[B]y intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were able to determine what television show an individual was watching.") (citing Dario Carluccio & Stephan Brinkhaus, *Presentation: "Smart Hacking for Privacy,"* 28TH CHAOS COMM. CONGRESS (Dec. 2011)).

350. Thomas K. Clancy, *The Fourth Amendment as a Collective Right*, 43 TEX. TECH L. REV. 255, 271 (2010).

351. There may well be a statutory check created, but none from a Fourth Amendment perspective. *See supra* notes 93, 106, 203.

352. Richards, *supra* note 32, at 1953 ("[T]he gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance. It might sound trite to say that 'information is power,' but the power of

protection of IoT information is consistent with the value society places in collective security over mass governmental intrusion.

IV.
DIGITAL CURTILAGE: REDEFINING EFFECTS IN THE INTERNET OF THINGS

The Article has argued that a space exists in Fourth Amendment doctrine for broadening the definition of "effects" to include the internal data and external communication signals of devices connected in the Internet of Things. It has also shown why this definition is consistent with Fourth Amendment language and principles. This Part seeks to operationalize this definition into a workable framework to analyze the contours and limits of this Fourth Amendment protection.

A. "Protect All Data" v. "Protect Internal Data" Approaches

From one perspective, because smart objects continually generate and share data, "effects" could be broadly redefined to include all of this information. In simple terms, a modern effect could include the physical object, the internal data, and the external communication signals because all are intrinsically part of the smart object. This "protect all data" approach offers the virtue of security and simplicity, but may upon further examination provide too much protection.

Take as an example a scenario in which police recover a smart pill bottle from a suspect prior to arrest.[353] Without a warrant, police have three obvious ways to investigate the contents of the pill bottle. First, they could be old-fashioned and open the container to discover the pills inside. Second, police could retrieve the stored, electronic data inside the pill bottle that would detail the types of pills and the frequency of use. Third, police could intercept the wireless signals coming from the pill bottle to the pharmacy (for refills) or the doctor's office (for monitoring medication) or to the person (for health monitoring). A "protect all data" approach would protect everything, redefining all this digital information as part of the effect itself.

This "protect all data" definition finds some support in arguments of security-privacy, property, constitutional interests, and common sense. From a traditional Fourth Amendment perspective, the physical object would be protected as a closed container.[354] After *Riley*, the internal, stored data in the

personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion.").

353. Rose, *supra* note 4, at 9 (describing the GlowCap as an "enchanted" object).

354. Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1414 (2010).

object likely would receive the same protection as the physical object.[355] Opening the bottle is arguably less intrusive than examining the data in the bottle (which might reveal a detailed and personal pattern of past pill taking, rather than just the pills left over). But what about the communication signals? Should communication data that might travel in packets of information to the drug store or around the world be considered part of the effect? What if the owner of the pill bottle took no steps to preserve the information from dissemination? What if the pill bottle had a store-installed communication chip that the owner did not even know was releasing the information? These harder questions counsel against a blanket "protect all data" approach.

More pointedly, these questions may necessitate drawing a distinction between the internal stored data in the thing and external transmitting data from the thing. A modification of the "protect all data" approach would be to protect only the stored internal data in the object. Internal data captured and stored in a smart device in the Internet of Things would be privileged and protected (requiring a warrant). The external communications signals would remain unprotected. This "protect internal data" approach offers a half measure to protect digital value embedded in a smart effect. The data is personal and likely something the owner wishes to exclude others from learning about. Further, because of the intrusive nature of recovering the data and because the smart data is integral to the thing itself, this redefinition offers a substantial (albeit not complete) measure of protection.

This solution however does not solve the hardest question about communication signals in the Internet of Things. In fact, it arguably only extends existing practice and law concerning smartphones, computers, and other digital containers to the problem of IoT stored data.[356] While the Supreme Court has not ruled directly on the issue (*Riley* arose in a search incident to arrest context), the conclusion that stored data in digital effects should be treated as part of the effect seems a logical extension of existing doctrine. The harder and more important question is whether the billions of sensor signals, which will soon be communicating all over the country, also should be considered part of the effect itself.

This Article proposes a cabined definition of a Fourth Amendment effect to include some, but not all of those data signals. Built around the metaphor of curtilage,[357] itself a legal fiction to expand the protected area around a

355. The Supreme Court in *Riley* appears to accept that a search of this digital information stored in an effect could be more invasive than physically searching the object itself. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

356. *See, e.g.*, Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 118 (2011); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 202–03 (2005).

357. California v. Ciraolo, 476 U.S. 207, 213 (1986); Catherine Hancock, *Justice Powell's Garden: The Ciraolo Dissent and Fourth Amendment Protection for Curtilage-Home Privacy*, 44 SAN DIEGO L. REV. 551, 553 (2007).

home,[358] the theory of "digital curtilage" provides a framework to define a new vision of a constitutionally protected digital effect. While admittedly a lesser protection than a "protect all data" approach, the theory also goes beyond merely protecting internal stored data.

B. The "Digital Curtilage" Approach

Digital curtilage is a theory that attempts to secure certain data from interception and surveillance. Building off a reclaimed property-based focus of the Fourth Amendment, but adapting that insight to the virtual world, digital curtilage creates a new space of constitutional protection. In defining this protective space, the theory also helps draw the contours of a Fourth Amendment search for data embedded in a smart device and signals emanating from a smart device.

As I have written before, curtilage provides a useful analytical metaphor because it "offers a historically grounded, constitutionally balanced, and flexible framework to understand the core protections of the Fourth Amendment."[359] Traditional curtilage recognizes that while many of our most private activities take place inside the home, they can also occur beyond the four walls of the actual homestead, and that this expanded space also deserves a heightened level of protection.[360] The Supreme Court has stated that Fourth Amendment "property" includes curtilage and offered the following definition of the protected area:

> [W]e believe that curtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by.[361]

Breaking down these factors, curtilage requires: first, a connection with the home; second, a claimed and marked space to exclude others (generally seen through enclosures and steps taken to prevent observation); and third, the use of this space which relates to personal or family activities (protecting "the

358. Erik Luna, *Drug Exceptionalism*, 47 VILL. L. REV. 753, 759 n.36 (2002) (describing curtilage as a legal fiction).

359. *See* Ferguson, *supra* note 27, at 1313.

360. United States v. French, 291 F.3d 945, 951 (7th Cir. 2002) ("This protection is not limited to the four walls of one's home, but extends to the curtilage of the home as well."); Tomkovicz, *supra* note 27, at 425 ("The tendency to discount informational privacy interests located outside dwellings seems misguided. If a domain harbors privacy interests entitled to protection against the physical intrusions known to our ancestors, those interests should also be shielded against technological surrogates.").

361. United States v. Dunn, 480 U.S. 294, 301 (1987).

privacies of life").[362] Each of these factors can be applied to an expanded vision of a Fourth Amendment effect through the theory of digital curtilage.

Under this new definition, digital curtilage denotes the expansion of an effect to include embedded data and certain communicating data signals beyond the physical object. Digital curtilage looks to define a "smart" effect to include: (1) data and signals that are closely associated with the effect; (2) data and signals that have been marked out and claimed as secure from others; and (3) data and signals used to promote personal autonomy, family, self-expression, and association. As will be evident, this proposed test will—like traditional curtilage—provide a fact-based and balanced Fourth Amendment protection. Courts applying a digital curtilage test will need to analyze each of the three factors.

1. Close Association with the Effect

Data stored on a smart effect is closely associated with the effect. To retrieve the data one needs to connect with the effect itself, thus demonstrating the close connection between information and object.

Data emanating from a smart effect is also closely associated with the effect. The data derives from a constitutionally protected interest—the physical effect itself—and, thus, benefits from this derivative protection. In the digital world, the "close" association is not a physical closeness. Physical proximity means less because of the fluidity of data to travel, duplicate, and overcome physical barriers. On a visceral level, there probably should be a difference between a police officer standing outside a hospital bed and intercepting health data and the same officer intercepting the data from the comfort of police headquarters. But from a technological level, the process and harm of interception remains virtually the same.[363] As a result, a pure physical proximity analysis does not mesh with existing technological reality.

For this reason, a metaphorical (or perhaps philosophical in the loose ontological sense) approach may provide a better understanding of closeness. Because smart data is part of the thing itself, and because the thing was designed to communicate smart data, then the data should be considered closely associated with the effect itself. Consumers buy the item because of its smart features. As discussed earlier, a smart bandage that monitors healing is

362. Oliver v. United States, 466 U.S. 170, 180 (1984) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)); *see also* Riley v. California, 134 S. Ct. 2473, 2495 (2014) (citing *Boyd* for "privacies of life"); *Ciraolo*, 476 U.S. at 212–13 ("The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened.").

363. Further, in the ordinary case neither the user of the device nor the officer nor an evaluating court would know the physical closeness of the data to the original device. In addition, there exists the reality that data from a smart device might be both in the device and transmitting from the device at the same time. Computers, unlike physical objects, can duplicate the information, share it, and thus data can coexist in both places at the same time.

not the same thing as an ordinary bandage. Consumers are paying for something extra (the monitoring), and thus they possess something extra. The data storage and use becomes a property right, which they can control. At a minimum, consumers should be able to exclude others from that digital property.[364] A strong claim can be made that communicating data from most smart effects should be considered "associated with" the effect, satisfying the first factor of the test. Data, like curtilage, derives derivative protection from the constitutionally protected source.

Under the first prong of a digital curtilage analysis this derivative connection will offer broad protection for both stored data and emanating data signals. Because the information comes from a smart device, the data will be considered a part of this smart device. In the same way the curtilage principle extends protection of the home outside the home, so digital curtilage extends protection of data outside the smart effect.

2. Marked and Claimed as Secure Factor

The second factor, requiring data and signals to be marked out and claimed as secure, will narrow the scope of protection for certain smart devices. Curtilage requires building a metaphorical wall around your house as a symbolic and practical expression of security.[365] By excluding others, you help define the markers of where you expect security.[366] In the technological realm, this exclusion can be observed through steps taken to preserve security. You can secure a Wi-Fi system through encryption.[367] Smart phones allow you to opt out of locational tracking and other sharing requests.[368] Companies are inventing other secure technologies almost daily.[369] Legal barriers can also be

364. Such a result is akin to the "protect all data" framework, because the smart effect (when acting as a smart effect) includes everything that causes the thing to be the thing.

365. *See* Amelia L. Diedrich, *Secure in Their Yards? Curtilage, Technology, and the Aggravation of the Poverty Exception to the Fourth Amendment*, 39 HASTINGS CONST. L.Q. 297, 300 (2011) ("As a means of defense in England's 'early times,' it was customary for home owners to surround their home and related buildings with a 'substantial wall.' The resulting area inside the wall and outside the home was known as the curtilage.").

366. Clancy, *supra* note 10, at 362 ("Defining security as having the right to exclude has historical roots and meaning; the Framers lived in a time that equated security with the ability to exclude. It provides an easily identified and applied rule designed to protect an individual's right to be safe as to his or her person, house, papers, and effects.").

367. Becky Waring, *How to Secure Your Wireless Network*, PCWORLD (Apr. 9, 2007, 1:00 AM), http://www.pcworld.com/article/130330/article.html [http://perma.cc/8WUM-Z2EZ]; *see also* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?"* 33 CONN. L. REV. 503, 504 (2001) (discussing whether encryption can create a reasonable expectation of privacy).

368. Dennis O'Reilly, *Simple Ways to Enhance Your Internet Privacy*, CNET (June 21, 2013, 1:07 PM), http://www.cnet.com/how-to/simple-ways-to-enhance-your-internet-privacy [http://perma.cc/NRZ8-H24J] (describing ways to opt out of locational tracking).

369. *See, e.g.*, Rolf Weber, *Internet of Things—New Security and Privacy Challenges*, 26 COMPUTER L. & SECURITY REV. 23, 26 (2010) (discussing security options); Timothy B. Lee, *My Smartphone, The Spy: Protecting Privacy in a Mobile Age*, ARS TECHNICA (Mar. 14, 2012, 11:00

created to protect data such as creating contractual or fiduciary relationships.[370]

This "marked and claimed as secure" factor requires an examination of how the creator of the data interacts with others seeking to collect data. Generally speaking, for stored data, because the information lives within the effect, a presumption of security exists. To retrieve information, an investigator would have to physically manipulate or hack into a device. While stored data might remain unencrypted or even unprotected, because of its location in an effect, it retains constitutional protection. This understanding merely extends existing law protecting stored data in smartphones, computers, etc.[371]

For communicating data, the question is a bit more difficult. If one chooses to secure data from others using technological means, then this affirmative act will be respected as signaling a desire for security. If one shares data without securing the information, then this choice (signaling a lack of concern with data security) will also be respected. The key is an affirmative act of securing the data both as a symbolic and signaling mechanism. Even if sophisticated hackers could thwart these types of security measures, a symbolic statement of security exists. After all, just because burglars and police can enter locked houses, it does not mean citizens lose a claim of security behind those walls. Thus, as long as the consumer takes some affirmative steps to claim security in the device, this factor has been satisfied. Under this step, courts will need to examine what actions were taken to mark and secure the data.

A real difficulty arises, however, because many objects in the Internet of Things do not provide the option of opting out or marking a claim of security.[372] Many sensors are not sophisticated enough to allow for consumer control.[373] By reason of cost and ubiquity, the sensors are developing without an emphasis on data security. While some home monitoring systems, smart cars, smartphones, and health devices have (or will soon have) options to secure the data and communications (through secure networks, opt-out

AM), http://arstechnica.com/business/2012/03/my-smartphone-the-spy-protecting-privacy-in-a-mobile-age/2 [http://perma.cc/4KBJ-PSEF].

370. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 103 (2004) (suggesting that personal data should be considered shared with third parties as in a fiduciary relationship, requiring heightened protection of data and greater restrictions to share data with others); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV 611, 649 (2015).

371. *See generally* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer*, 75 MISS. L.J. 193, 196 (2005); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 550 (2005).

372. Brill, *supra* note 110, at 211–12, 216 (discussing the need to design IoT devices for consumer control).

373. *Id.* at 216; Atzori et al., *supra* note 38, at 2801 ("[M]ost of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security.").

provisions, or the like), other sensors do not.[374] This lack of choice and resulting lack of security presents a real problem with the early iteration of the Internet of Things. If one cannot mark out a space by opting in or opting out—and thus controlling access to one's data—the virtual wall will not hold. In fact, consumers may not even know these ubiquitous sensors are tracking them.[375] This problem of unknowing self-surveillance will reduce the number of objects protected by the Fourth Amendment under the digital curtilage theory.

The hope is that at least with devices that collect sensitive personal data, some technological mechanism will be designed to allow consumer control of the information. The further hope, of course, is that a focus on effects will spur the technological developments to ensure the ability to make a claim of security for communicating data. Today, one might be able to turn a smartphone into private mode, but in the future a digital curtilage mindset might create an entire operating system or application designed to allow consumers to protect data from interception.

3. Nature and Uses: Personal and Family Interests Factor

Finally, the third factor looks at how the data from an object is used by the owner. Analyzing the nature and use of data coming from personal effects will further refine or limit the protections afforded to effects.[376] Sensors in the Internet of Things can be found in all sorts of commercial and consumer devices. A focus on data and signals from objects linked to personal or private matters will limit the expanded definition of an effect.

Protecting only personal and family-use data is consistent with the intent of traditional, physical curtilage. In order to protect the sanctity of the home, curtilage protected areas that encouraged home-like activities. In physical curtilage, such protections might include most self-expressive (what one says, does, or thinks), associational (who one associates or communicates with), familial (what one's family does), and other personal revelations (matters of

374. *See, e.g.*, Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J. (Nov. 18, 2014, 10:30 PM), http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801 [https://perma.cc/B75F-QRXU]; Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data*, WASH. POST (May 19, 2015), https://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html [https://perma.cc/TTX6-JNAD]; Daan Pepijn, *Internet of Things: Security, Compliance, Risks and Opportunities*, BUSINESS (Nov. 6, 2015) http://www.business.com/technology/internet-of-things-security-compliance-risks-and-opportunities [https://perma.cc/J42K-AVN6].

375. Weber, *supra* note 369, at 24 ("The attribution of tags to objects may not be known to users, and there may not be an acoustic or visual signal to draw the attention of the object's user. Thereby, individuals can be followed without them even knowing about it and would leave their data or at least traces thereof in cyberspace.").

376. Oliver v. United States, 466 U.S. 170, 180 (1984) (defining curtilage as "the area to which extends the intimate activity associated with the 'sanctity of a man's home'").

faith, health, lifestyle). Similarly, in the digital context, this understanding would protect expressive, associational, religious, family, personal, and dignity interests as opposed to unrevealing or impersonal data. For example, a smart t-shirt that monitors a heartbeat will be more protected than a smart muffler that monitors car exhaust. That said, the "privacies of life" (the language referenced in *Boyd*, the curtilage cases, and *Riley*)[377] can and did include participation in illegal or otherwise antisocial behavior. The Founders were largely concerned with protecting against customs agents investigating their avoidance of taxes as they fomented the intellectual basis for revolution. As a result, the Fourth Amendment has been read to encourage an expansive vision of human development free from governmental surveillance. Thus, the personal and family interest argument should not be seen as a content-based test, but merely a recognition that many of the things we do (with or without smart objects) are done for personal growth and development.

While at first blush this distinction might seem arbitrary, it is the same type of distinction that separates a protected curtilage space from an unprotected open field.[378] Constitutionally protected interests are not just determined by property concepts (where you are standing) but also by privacy values and concerns about human autonomy that inform these conceptions of property (what you could be doing in that space).[379] To go back to Professor Davies's earlier insight, originally the Fourth Amendment "was understood to provide clear protection for houses, personal papers, [and] *the sorts of domestic and personal items associated with houses, and even commercial products or goods that might be stored in houses*."[380] Thus, not all property was treated the same, with protected effects originally understood to include more personal or familial items. In fact, as Maureen Brady has discovered, the founding generations' effects tended to be those items associated with religious or cultural self-expression.[381] This same conception can be applied to the modern world as many new smart items are merely enhanced versions of ordinary, personal objects. Domestic objects and associated data will be more protected than objects that have little connection to personal autonomy, family, or other traditionally private matters.

Again, in the balancing required by a digital curtilage theory, courts will need to draw fine lines. Some judges may well find particular objects more protected than others. Much will come down to a judge's determination of

377. *See id.* at 179 ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance.").

378. *Id.*

379. Stern, *supra* note 207, at 940 ("Privacy of intimate association disregards the physical home in favor of assessing the likelihood that search activity will disrupt domestic life, engender interpersonal conflict, reveal personal information that is private to and constitutive of relationships, and chill socialization and intimacy.").

380. Davies, *supra* note 134, at 714 (emphasis added).

381. *See* Brady, *supra* note 129.

whether the data at issue implicates personal uses consistent with the idea of curtilage. Claims of security will need to be litigated. Arguments about steps taken to protect data, personal uses, and the like will be contested. But, as with traditional curtilage, judges will now have a framework under which to consider the competing values and tradeoffs of security, privacy, law enforcement, and liberty.

4. Final Thoughts

The theory of digital curtilage offers a framework to expand the definition of a Fourth Amendment effect beyond the physical object to include embedded data and some communication signals. Admittedly a legal fiction, digital curtilage provides a test to protect certain data and signals based on traditional Fourth Amendment values. The theory fills the doctrinal gap even if it does not provide absolute protection to all data and signals in the Internet of Things.

Two important issues remain to be addressed. First, who owns the data in the Internet of Things? Second, what should courts make of the distinction between metadata and data in the Internet of Things? Both subjects are largely beyond the scope of this Article, but I offer brief answers.

Ownership issues of personal data are only just being addressed and debated in the digital world.[382] Information about my heartbeat recorded in a Fitbit is my personal data, but it is also being shared with the company that sold me the device. It is my heartbeat information, but a company's intellectual property.[383] Can I make a claim to secure this data against interception? For Fourth Amendment purposes, the answer is yes. While I cannot control what the company does with the information, I can still claim control over the data vis-a-vis the government. Any police interception of my data directly from me would implicate my constitutional rights. Just as the purchaser retains constitutional protection in rented cars, hotel rooms, phone booths, and borrowed pairs of slacks, I retain a claim not to have relinquished all security just because someone else also has access to the data. The fact that I share access to my hotel room with the hotel maid does not mean I also have granted police permission to search my room. While the contours of this ownership remain unresolved (and distorted by the third-party doctrine), the fact that other people can claim ownership of the data does not detract from the data owner's ability to exclude others from direct access to the data.

382. *See* Fairfield, *supra* note 330 (proposing a new form of intellectual property protection modeled on block chain technology).

383. *Id.*; Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1201 (2000) (describing the relationship between intellectual property and privacy interests).

Courts have not resolved the question of whether metadata[384] deserves lesser protection than other data. Old-fashioned types of metadata like pen registers, which can reveal telephone contacts but not telephone content, have been held to be outside the Fourth Amendment's protection.[385] Similarly, in the national security context, courts have deemed some bulk collection of communications metadata analytically distinct from content collection.[386] However, in the context of the Internet of Things, the contacts-content distinction largely blurs. First, the line between data and metadata in the context of billions of connected things becomes vanishingly thin. Metadata can reveal personal information just like content.[387] Metadata about the number of times a particular license plate travels down a particular road might reveal the content of the travel (if, for example, the road led to a mosque). Second, in many ways the Internet of Things is really the "internet of metadata" with the collection of data trails being so ubiquitous and constant that their creation maps our lives. Thus, as a general matter, this Article would not endorse a metadata-data distinction of any real consequence.

Yet, metadata may result in a different level of protection under a digital curtilage theory. Applying each of the three analytical components—(1) close association with the effect, (2) marked or claimed as secure, and (3) personal-family uses—metadata may have a weaker claim to Fourth Amendment protection.

Metadata, like content data, can claim equal derivative protection from the effect. The data comes from the effect, so the first factor presents no materially different analysis.

Second, similar to content data, the level of security depends on the object. The digital curtilage theory requires some marking of security and likely a good percentage of existing metadata fails this prong. Sophisticated technology users will adapt to this requirement, masking or blocking certain metadata transmissions. Most people, however, live unaware of the data trails left behind through metadata and thus would not know enough to build a

384. Metadata refers to data about data, namely how and when it was created or modified, or information about how the data connects to other data. In the world of smart devices, metadata covers the largely unseen tracking points of geo-location, types of devices used, and the time, recipient, and contacts of information sent. Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 646 (D. Kan. 2005) ("[Metadata is] information describing the history, tracking, or management of an electronic document.").

385. Smith v. Maryland, 442 U.S. 735 (1979).

386. David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209, 241 (2014).

387. Jane Mayer, *What's the Matter with Metadata?*, NEW YORKER (June 6, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html [http://perma.cc/SM7H-VMRR]; Geoff Nunberg, *Calling It 'Metadata' Doesn't Make Surveillance Less Intrusive*, NPR (June 21, 2013, 1:25 PM), http://www.npr.org/2013/06/21/193578367/calling-it-metadata-doesnt-make-surveillance-lessintrusive [http://perma.cc/8WRC-XESA].

virtual wall. In addition, the seduction of convenience (of having things automated and helpful) will convince some people to tear down existing virtual walls. In many cases, the tradeoff for convenience requires revealing metadata to collecting sensors. Metadata left unguarded would not be protected by the digital curtilage theory.

The final factor will be whether the metadata reveals some personal-family interests traditionally protected by curtilage. Metadata reveals many associational relationships, patterns, and even personal activities.[388] Both *Jones* and *Riley* hint that the Supreme Court sees this aggregation of personal geolocational data as something that could implicate traditional Fourth Amendment considerations. As the Internet of Things grows in sophistication, so does the risk that similar, aggregated, personal information will be revealed. Thus, in determining whether metadata from a smart device reveals personal information, a court will need to weigh what interests are revealed by the data. The more personal the information, the stronger the argument for protection under a digital curtilage theory.

C. Redefining Searches of Effects in the Internet of Things

The foregoing analysis semantically and theoretically redefines a Fourth Amendment effect to cover the internal data and external communications of an object connected to the Internet of Things. Under a digital curtilage theory, if the object, data, and some signals were redefined as a Fourth Amendment effect, then the physical or virtual collection of data from the effect would be a search for Fourth Amendment purposes. Essentially, the expansion of the definition of an effect expands the threshold of what is being searched.

This threshold step is necessary, but not sufficient to answer the question of whether a Fourth Amendment search has occurred. The second step looks to see if a physical or virtual intrusion of this constitutionally protected space constitutes a Fourth Amendment search. As to physical intrusion, consistent with current law, the physical acquisition of internal data presents a rather straightforward analysis. After *Jones*, physical interference with the effect to obtain information would be a search.[389] If the officers used a device directly to download the data on a portable drive, this would be a physical intrusion of a constitutionally protected space with the intent to obtain information—the definition of a search in *Jones*.

The question is less clear with a virtual acquisition (i.e., a law enforcement officer virtually hacking into the stored data in the device using code-breaking techniques akin to hacking into a computer). The argument here

388. Dahlia Lithwick & Steve Vladeck, *Taking the "Meh" Out of Metadata*, SLATE (Nov. 22, 2013, 12:07 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html [https://perma.cc/R84N-NC9S].

389. *See supra* Part II.C.1.D.i

is that a virtual acquisition of the same data should lead to the same result.[390] If police virtually hacked into the stored data without touching the device,[391] the harm is the same, the intent is the same, the collection is the same, and the Fourth Amendment principles are largely the same. True, police have not touched the device, but they have interfered with the property, privacy, and security interests in the effect. As others and I have written, this technologically assisted intrusion should be considered the same as a physical intrusion.[392] The harm of searching a computer is not simply touching the keyboard, but invading the digital materials inside the device. Or borrowing from the facts in *Jones*, if the police had virtually hacked into the data in Mr. Jones's car, recovering 28 days' worth of geolocational data, a similar harm would exist as physically planting a GPS device. The data is within the effect and virtually acquiring it presents the same intrusion. Or in *Riley*, if the police had virtually hacked the phone and read through the same information, the Fourth Amendment reasoning should not be different. The security of the effect has been violated.

Similarly, acquisition of communications signals also should be protected if the signals fall within the redefined protection of digital curtilage. By expanding the definition of a Fourth Amendment effect to include stored data and communication signals, the theory of digital curtilage would also protect against interception of that data and signals by virtual means. A constitutional wall has been built to keep out physical and virtual acquisition of otherwise personal data.

In *Kyllo*, the Supreme Court considered the logic of such technologically enhanced information capturing: "We think 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

390. Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1243 (2012).

391. LORI ANDREWS ET AL., INST. FOR SCI., LAW & TECH., DIGITAL PEEPHOLES: REMOTE ACTIVATION OF WEBCAMS, TECHNOLOGY, LAW AND POLICY 7 (2015), http://www.ckprivacy.org/uploads/4/1/8/3/41830523/digital_peepholes_2015.pdf [https://perma.cc/6FHA-KUG8] (discussing the technology that allows individuals to virtually hack into computers from remote locations).

392. Ferguson, *supra* note 27, at 1338; Erica Goldberg, *How* United States v. Jones *Can Restore Our Faith in the Fourth Amendment*, 110 MICH. L. REV. FIRST IMPRESSIONS 62, 68 (2012) ("Justice Scalia's rationale, if updated to consider electronic penetration a form of trespass, would permit the labeling of more intrusions as searches, whether they look like traditional trespasses or modern-day, electronic trespasses."); Tomkovicz, *supra* note 27, at 433 ("It is not implausible to contend that when the authorities use technology to access publicly-situated and physically-exposed details that otherwise would not or might not be perceptible to human faculties they violate privacy. If the exploitation of a device enables the government to learn details that could not or would not have been learned at all by means known to the Framers, not even by methods subject to constitutional regulation, categorical rejection of a privacy claim based on 'public location' does not seem sensible.").

protected area' constitutes a search."[393] As Professor Thomas Clancy has written, "The logic of *Kyllo*'s analysis should be extended to all of the objects protected by the Amendment—houses, people, papers, and effects."[394] This would certainly include virtual interception of the data inside the smart objects, but should also include their transmitting signals. Just like the heat emanating from the house in *Kyllo*, the communication signals emanating from an IoT device in the home should be protected because interception infringes the constitutionally protected thing itself.

D. Objections to Considering Internal Data and External Communication Signals as Fourth Amendment Effects

Any theory that purports to redefine a constitutional term of art in use since 1791 may invite a few objections. This Section addresses the two obvious concerns with digital curtilage and the idea of extending the definition of effects to include the internal data within a smart effect and external signals emanating from the smart effect. First, is digital curtilage better than the existing Fourth Amendment protection we currently maintain under a reasonable expectation of privacy theory? Second, is it a workable theory such that courts can use and apply it with some measure of consistency? Both of these concerns—efficacy and utility—will be addressed in turn.

1. Efficacy

As set out in Part II, significant gaps exist in current Fourth Amendment doctrine allowing for virtual acquisition of stored data in smart objects, and interception of communication signals coming from smart objects. Neither involves a physical intrusion of any kind (*Jones*), and neither would be automatically protected by a reasonable expectation of privacy under current cases (*Katz*). One could, however, argue that the solution is not to redefine the effect as proposed under a digital curtilage theory, but merely to expand the reasonable expectation of privacy test to include these previously uncovered areas.

The question then becomes, why is redefining an effect better than redefining an expectation of privacy? The answer turns on four considerations. First, in an era of ubiquitous sensor surveillance, privacy—as a defining concept—may not provide much protection. The Internet of Things itself is helping to erode traditional spheres of private space by making information about those private spaces more publicly available than before. If you have chosen to use a smart object to reveal some personal information about yourself to others, a claim of personal privacy does not seem to be the strongest

393. Kyllo v. United States, 533 U.S. 27, 34 (2001).

394. Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 38 (2006).

argument. As mentioned, "security" with its emphasis on the ability to exclude others, and its connection to property, may be a stronger conceptual framework on which to base Fourth Amendment protections. A digital curtilage theory based on the concept of security thus avoids this pure privacy framework. While neither privacy nor security offers a perfect fit, the latter provides more protection against growing surveillance technologies that take advantage of our desire to turn private activities into shared data.

Second, and relatedly, expectations shift, so what we collectively expect to remain private may change over time. As other scholars have argued, a theory based on expectations can be undermined by redefining those expectations in a public manner.[395] As can be seen in the debates between the Justices in *Jones*, new surveillance technologies pose real privacy risks with no settled expectations.[396] We all know we are being surveilled in public through cameras, license plate readers, and the like, but we are also uncertain about how we should react to that surveillance. If the government mandates a black box data recorder in every new car, shouldn't that impact our expectations of privacy about how we drive? The fact that we do not know the answer to these questions raises a concern with leaving the future to the expectation of privacy standard.[397] While digital curtilage may produce its own questions, the theory does not turn on societal expectations as much as individual actions. Individuals can claim a space of security, and in doing so take more control over the data from their personal effects.

Third, expectations of privacy tend to be divined through ex post determinations from a court,[398] which limits individual control over those spaces. If we require a court to decide our collective expectations, we shift the power of decision away from the people and to the courts. The Fourth Amendment is not alone in being a judge-defined right, but if we cannot know the expectations until a majority of the justices tell us what they are, citizens become disempowered from even trying to claim the right. Again, digital curtilage places the initial onus on the individual to assert a right of security against others and the government. While, of course, such a claim might eventually be rejected by a majority of justices, the power to assert the claim

395. *See generally* Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195 (2008); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

396. Kerr, *supra* note 95, at 326.

397. *But see* 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 (2015).

398. Christopher Slobogin, *An Empirically Based Comparison of American and European Regulatory Approaches to Police Investigation*, 22 MICH. J. INT'L L. 423, 454 (2001) (identifying the problem of judicial hindsight bias in evaluating the justification for police searches); Slobogin & Schumacher, *supra* note 395, at 765–68 (demonstrating how hindsight bias impacted determinations of an expectation of privacy).

still remains with the people. Even if the ultimate outcome remains the same, the power to control the right has shifted, giving the people more involvement in the process to establish Fourth Amendment freedoms.

Finally, the third-party doctrine remains a significant barrier for the robust protection of personal data. Under existing law, sharing data with a third party undercuts any expectation of privacy in that data. The digital curtilage theory, based on property insights and conceptions of security rather than privacy, provides greater protection. While the lines around digital curtilage have yet to be drawn, the framework exists to create more protection for personal data. As courts look to move past the third-party doctrine, the theory of digital curtilage provides a nonprivacy-based alternative.

2. Utility

Assuming that a digital curtilage theory may be necessary to fill some of the gaps in the current Fourth Amendment doctrine, a corollary question arises: whether the proposed framework can be made useful to courts defining the contours of a Fourth Amendment effect. Admittedly, a multifactor test that incorporates judgments about constitutionally appropriate interests and analyzes family or autonomy interests runs against the Supreme Court's preference for "bright-line" Fourth Amendment rules.[399]

Two arguments respond to this concern. First, the proposed test is no more complicated than the existing tests to determine a reasonable expectation of privacy or to define curtilage. The case-by-case approach might well turn out to be a virtue and not a vice for judges needing to make difficult calls. Multifactor tests have regularly been adopted in the Fourth Amendment context.[400] Curtilage is just one example of a structured test that controls the analysis but not the outcome. Courts are used to considering factors and totalities when it comes to a reasonableness analysis. Judges prefer discretionary powers, and this type of multifactor test provides that ability to determine the contours of the Fourth Amendment on a case-by-case basis.

Second, this type of case-by-case approach might well provide the opportunity to shape the technology. If, for example, the courts began requiring an affirmative signaling of security (through an opt-out button or encryption), then designers might design things in the Internet of Things to meet this standard.[401] If courts began protecting only marked personal data coming from

399. *See generally* Wayne R. LaFave, *The Fourth Amendment in an Imperfect World: On Drawing "Bright Lines" and "Good Faith,"* 43 U. PITT. L. REV. 307, 321 (1982) (describing the need for Fourth Amendment rules that police officers can easily apply).

400. Generally, the Court favors bright-line rules for police officers and remains comfortable with balancing tests for judges. Albert W. Alschuler, *Bright Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227, 227–31 (1984); Maclin, *supra* note 303 (discussing the Court's preference for bright-line rules).

401. In fact, the encryption debate over the Apple iPhone supports this security by design argument. *See* Brian Naylor, *Apple Says iOS Encryption Protects Privacy; FBI Raises Crime Fears*,

an effect, we might start seeing certain consumer products that specifically advertised this protection (e.g., Fourth Amendment-compliant pill bottles). In the future, the Internet of Things may need to be consciously designed to take into consideration security of the data embedded and shared with other sensors.[402] Such security by design, influenced by a legal framework, would ultimately influence the larger architecture of the Internet of Things.[403]

The open question is how responsive technology will be to the law. Until the average consumer becomes more Fourth Amendment-focused, security concerns may not drive technological innovation. While beyond the scope of this Article, the current debate over secure default encryption—developed by companies to avoid legal requests by law enforcement—provides one example of how technology companies may encourage a culture of data security in response to legal changes.[404] The same debate may soon also develop around smart devices connected in the Internet of Things.

CONCLUSION

This Article has demonstrated that the Fourth Amendment's language can—without distortion to Fourth Amendment principles—incorporate a modern understanding of "effects," similar to how the word "homes" has expanded to include curtilage, and the word "persons" has expanded to include corporations. This minor change in definition would have a major impact if the "constitutionally protected spaces" language continues to influence analysis of future Fourth Amendment cases, as it has in *Jones* and *Jardines*.

The Internet of Things has just begun to shape our lives, and Fourth Amendment jurisprudence will need to adapt. If billions of sensors filled with personal data fall outside of Fourth Amendment protections, a large-scale

---

NPR: ALL TECH CONSIDERED (Oct. 8, 2014, 5:17 PM), http://www.npr.org/blogs/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears [http://perma.cc/D4QN-K78R].

402. FED. TRADE COMM'N, *supra* note 349.

403. Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 992 (2012) ("The call for privacy by design—the practice of embedding privacy protections into products and services at the design phase, rather than after the fact—connects to growing policymaker recognition of the power of technology to not only implement, but also to settle policy through architecture, configuration, interfaces, and default settings."); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 430–31 (2014) ("The basic idea of Privacy by Design is that privacy cannot be ensured solely by regulatory oversight by government agencies; instead, effective protection of privacy also requires companies to respect the privacy of individuals by making privacy protection an ordinary but integral part of the way they do business.").

404. David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES (Sept. 26, 2014), http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html [https://perma.cc/7KD3-HHHU]; Andrea Peterson, *Privacy Is Tech's Latest Marketing Strategy*, WASH. POST: THE SWITCH (Sept. 26, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/26/privacy-is-techs-latest-marketing-strategy [https://perma.cc/P8ZY-B3ES] (describing the marketing of products to appeal to privacy concerns).

surveillance network will exist without constitutional limits. Redefining effects to protect IoT data is a necessary step toward providing a measure of protection. While not without its own questions, the theory of digital curtilage offers a grounded, balanced, and useful framework to harmonize the Internet of Things and the Fourth Amendment of effects.