THE "SMART" FOURTH AMENDMENT

Andrew Guthrie Ferguson†

"Smart" devices radiate data, exposing a continuous, intimate, and revealing pattern of daily life. Billions of sensors collect data from smartphones, smart homes, smart cars, medical devices, and an evolving assortment of consumer and commercial products. But, what are these data trails to the Fourth Amendment? Does data emanating from devices on or about our bodies, houses, things, and digital devices fall within the Fourth Amendment's protection of "persons, houses, papers, and effects"? Does interception of this information violate a "reasonable expectation of privacy"?

This Article addresses the question of how the Fourth Amendment should protect "smart data." It exposes the growing danger of sensor surveillance and the weakness of current Fourth Amendment doctrine. The Article then suggests a new theory of "informational curtilage" to protect the data trails emerging from smart devices and reclaims the principle of "informational security" as the organizing framework for a digital Fourth Amendment.

† Professor of Law, UDC David A. Clarke School of Law. Thank you to my colleagues at the 2015 Privacy Law Scholars Conference who suggested this data-focused approach to the Internet of Things. Thank you also to the faculty at the University of Miami Law School and the Elon University Law School for helpful comments and suggestions.

INTRODUCTION

"Smart" devices radiate data.[1] From smartphones, fitness trackers, enchanted pill bottles, smart cars, and even smart refrigerators, these objects create extensive data trails revealing personal information, patterns, and activities.[2] But,

---

1 "Smart device" is a generic term for digitally enhanced objects that allow communication between the object and a sensor device. *See generally* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641–45 (2015) (describing development of smart things, smart people, and smart spaces).

2 *See infra* Part I.

what are these data trails for Fourth Amendment purposes? Are they part of the "persons," "houses," "papers," or "effects" mentioned in the Fourth Amendment's text?[3] Does interception of such data violate a person's reasonable expectation of privacy?[4] Do data trails simply fall outside of the Fourth Amendment's protection?

Part commodity, part property, and part expression, this smart data has become quite valuable to commercial marketers who track us for consumer purposes.[5] For law enforcement, such data trails will be similarly valuable to track and investigate suspects involved in criminal activity.[6] Geolocation can undermine an alibi or tie a suspect to a crime scene.[7] Health data can report elevated blood pressure consistent with drug use or physical assault.[8] A Ford automotive executive once admitted, "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."[9] The revealing power of smart devices for law enforcement will only continue to grow in sophistication and scope as more and more devices become connected via the "Internet of Things."[10]

---

3 The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

4 *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

5 Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 93 (2014).

6 Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936, 1940 (2013) (recognizing that the Internet of Things will subject "previously unobservable activity to electronic measurement, observation, and control").

7 *See, e.g.*, United States v. Jones, 132 S. Ct. 945 (2012) (involving the tracking of a narcotics suspect via a GPS device attached to his car).

8 Peppet, *supra* note 5 ("[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.").

9 Jim Edwards, *Ford Exec: 'We Know Everyone Who Breaks the Law' Thanks to Our GPS in Your Car*, BUS. INSIDER, (Jan. 8, 2014, 8:16 PM), http://www.businessinsider.com/ford-exec-gps-2014-1#ixzz3f7sNp0s8 [https://perma.cc/DXV2-XJCU]; *see also* Stephen E. Henderson, *Our Records Panopticon and the American Bar Association Standards for Criminal Justice*, 66 OKLA. L. REV. 699, 705 (2014) (observing that car manufacturers such as Ford are not the only ones accumulating data while you drive).

10 The term "Internet of Things" was coined by Kevin Ashton. *See* Kevin Ashton, *That "Internet of Things" Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/view?4986 [https://perma.cc/R9S3-LEC8]; *see also* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1599 (2014) ("The 'Internet of

The resulting web of sensors raises difficult questions about what data trails are for Fourth Amendment purposes. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[11] So the question becomes, is the data trail from an implanted "smart" heart monitor protected as part of the "person" as understood in the Fourth Amendment? Is the engine data emitting from a smart car analytically distinct from the "effect" that is the car? Is a digital business record any different from the physical document that might otherwise fall under the "papers" protection of the Fourth Amendment? Do these data streams deserve protection under a "reasonable expectation of privacy theory"[12] or some other theory?

This Article examines the question of what smart data is for Fourth Amendment purposes. This question matters because "what something is" and "where it is located" are fundamental to answer the threshold question of whether there has been a Fourth Amendment search.[13] Data—the ones and zeros of binary code—have been the subject of some jurisprudential exploration when it lies stored within a computer, smartphone, or other electronic device.[14] Data trails—the emitting digital in-

---

Things' is the newest wave in ubiquitous computing, a term used to describe the array of internet-enabled devices (like cars and traffic lights but also coffee pots and clothes) that are entering our everyday lives. These devices not only collect increasingly specific personal information; but they also can share that data with other people and other devices."); Neil Gershenfeld & JP Vasseur, *As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things*, FOREIGN AFFAIRS, Mar./Apr. 2014, at 60, 64–65, http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/as-objects-go-online [http://perma.cc/2EMP-EXKL]; 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/EE2L-49QD].

11 *See* U.S. CONST. amend. IV, *supra* note 3.

12 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

13 *See* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 324–26 (2002) (discussing the importance of threshold determinations).

14 *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2480–81 (2014) (smartphones); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (e-mail); United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008) (computer), *amended by and reh'g denied*, 533 F.3d 1003 (9th Cir. 2008); United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("A cell phone is similar to a personal computer that is carried on one's person . . . ."); United States v. Romm, 455 F.3d 990, 994 (9th Cir. 2006) (laptop); United States v. Carey, 172 F.3d 1268, 1270 (10th Cir. 1999) (computer); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (holding that the "Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects"). *See generally* Orin S. Kerr, *Searches and*

formation or signals from smart devices—have not been similarly discussed. Yet, because this information contains continuous, private, and revealing insights about our daily lives, these data trails may be as sensitive as stored data. If data trails lie outside the Fourth Amendment, then law enforcement can track this revealing network of information without any constitutional limit. If data trails are protected by the Fourth Amendment, a new constitutional framework needs to be developed to define this protection.

This Article proposes a response to the rise of "sensorveillance"—the ever-increasing ability for surveillance technologies to track individuals through the data trails they leave behind.[15] According to recent predictions, by the year 2020, between 50–75 billion devices worldwide will be connected by the Internet of Things.[16] Many of those American smart devices will be built within our homes, cars, personal property, and even implanted in our bodies.[17] By design, each of those smart devices will reveal digitized information about the user, and will be networked in an ever-growing web of sensors and collection systems. Some devices will be relatively sophisticated, encrypted sensors. Other devices will be cheap, unprotected sensors. Many will be interoperable, and others automatic, usually emitting data without the user's knowledge or control. But, all of them raise fundamental Fourth Amendment questions of how to protect personally revealing digitized clues about an individual's actions and life patterns.

Seizures in a Digital World, 119 HARV. L. REV. 531, 542 (2005) (noting that computers store "a tremendous amount of information that most users do not know about and cannot control").

15 The term "sensorveillance" owes its inspiration to the term "dataveillance." M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN. ST. L. REV. 809, 822 (2010) ("Richard Clarke coined the term 'dataveillance' to describe the systematic observation, collation, and dissemination that modern computing make possible."); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 33 (2004) (describing dataveillance as "a method of watching not through the eye or the camera, but by collecting facts and data"); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 270–73 (2008) (describing data mining practices of private companies).

16 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 [https://perma.cc/BWT2-GV36] ("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 . . . .").

17 *See infra* Part I.

The Supreme Court has only begun to explore the question of whether the Fourth Amendment needs a new digital understanding. In *Riley v. California*, the Court wrestled with the status of data in smartphones searched incident to arrest, providing early hints of how digital information should be treated under the Fourth Amendment.[18] Similarly, in *United States v. Jones*, five concurring Justices recognized the need to protect long-term, aggregated, geolocational data trails obtained through warrantless GPS surveillance.[19]

This Article seeks to expand on these tentative first steps and examine how data trails from smart objects should be considered under the Fourth Amendment.[20] This Article has three major goals. First, the Article seeks to situate the discussion of smart data in a larger discussion of "sensorveillance"—the rise of new surveillance technologies built within a networked world. Second, the Article seeks to explore the potential coverage and practical gaps of current Fourth Amendment doctrine as applied to the problem of data trails. Third, the Article offers a new theory "informational curtilage" as a workable analytical framework to approach data trails under the Fourth Amendment.

In examining the problem of data trails, this Article highlights that the Fourth Amendment—at its core—protects "informational security," as much as persons, property, papers, or privacy.[21] Underlying the protection of persons, papers, homes, and effects and behind the expectation of privacy lies a desire to guard personal information from government intrusion. In other words, it is not the corporal person, alone, that deserves protection, but also the information about the person. It is not the sheaf of papers, but the revealing personal details in those words that matter. It is not the physical home that is as important as what happens in the home. Data trails, because they are pure information, crystalize this insight. While privacy scholars and Fourth Amendment scholars have recognized this reality,[22] informational security has not registered

---

18 134 S. Ct. 2473 (2014).

19 132 S. Ct. 945 (2012).

20 In a companion article, I approach the same puzzle of how to apply the Fourth Amendment to the Internet of Things from a "thing-based perspective." *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 809–11, 825 (2016).

21 *See infra* Part III for a definition and examination of "informational security."

22 *E.g.*, James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 667 (1985) ("The constitutional text, structure, and history, as well as early fourth

significantly in Supreme Court cases or lower court judicial analysis. This Article begins the process of reclaiming this insight by focusing on the problem of pure data trails among the Internet of Things.

Part I of the Article details the development of the Internet of Things. While still in its infancy, the rise of new surveillance techniques through cheap and ubiquitous sensors is growing across the technological landscape. From the Internet of Things to the "Quantified Self," data trails offer new ways to investigate and monitor individuals suspected of crime. Part II of the Article examines the gaps in existing Fourth Amendment doctrine. As currently applied, the legal framework does not answer the question of data trails from smart devices. While insights and arguments can be drawn from precedent, real gaps remain. Part III of the Article argues that despite the gaps, a strong argument can be made to protect certain data trails among the Internet of Things. By examining the commonalities of why certain objects, places, and things are constitutionally protected, this section argues for a new protection based on the concept of informational security. Part IV operationalizes that argument into a new theory of "informational curtilage," that builds off a traditional Fourth Amendment concept of physical "curtilage."[23] This theory offers a solution to the challenges of sensorveillance and provides a conceptual framework to resolve other gaps in existing Fourth Amendment doctrine.

---

amendment cases, support the conclusion that the main reason for constitutionalizing informational privacy is its *instrumental* role as a medium within which other rights and interests can survive, even flourish."); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 492–94 (1990) ("[I]t is useful and appropriate to speak of [F]ourth [A]mendment restraints on government action in particular cases as expressions of the constitutional right to informational privacy."); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 740 (1989); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2058 (2004); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1659–66 (1999); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (2001).

23 *See infra* Part IV.

I
"SMART" DEVICES AMONG THE INTERNET OF THINGS

"Smart" devices communicate data to sensor systems designed to collect information.[24] Smart devices include sophisticated, computer-like handheld devices (iPhones, tablets) and simple, single-use RFID chips (clothing tags).[25] Smart systems can include large-scale, interconnected industrial infrastructure capable of running a major manufacturing plant[26] or free-floating "smart dust" the size of actual dust particles.[27] But, whether big or small, simple or sentient,[28] these smart things all create and communicate data designed to be collected by other smart things. This section briefly describes the growth and promise of smart devices among the "Internet of Things"[29] and then describes the potential perils of sensor surveillance.

---

24 No single agreed-upon definition exists about the term "smart device." Used here, the term signifies a generic device that has digital communication capabilities with other sensors.

25 Smart devices can include smart computer-like devices such as iPads, iPhones, Kindles, Apple Watches, etc. RFID chips involve a much lower capacity sensor with much fewer capabilities. 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. 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.").

26 Chloe Green, *The Internet of Things Business Process Revolution*, INFORMATION AGE (Sept. 10, 2014), http://www.information-age.com/it-management/strategy-and-innovation/123458453/internet-things-business-process-revolution [https://perma.cc/2F5Q-SF6A].

27 John D. Sutter, *'Smart Dust' Aims to Monitor Everything*, CNN (May 3, 2010, 8:27AM), http://www.cnn.com/2010/TECH/05/03/smart.dust.sensors/index.html [https://perma.cc/SE6E-FHC5]; Rebecca Rubin, Note, *Smart Dust: Just A Speck Goes A Long Way in the Erosion of Fundamental Privacy Rights*, 15 J. High Tech. L. 329, 342 (2015) ("The Smart Dust project, created by researcher Kris Pister in the 1990s, reflects his previously only-imagined idea of a world of constant monitoring through the use of countless tiny sensors sprinkled upon the Earth. Pister . . . created smart dust, a micro-millimeter scale technology capable of both military and commercial application for sensing vibrations, temperatures, sounds, and lighting, among other elements.").

28 Richard L. Rutledge et al., *Defining the Internet of Devices: Privacy and Security Implications, Georgia Institute of Technology Technical Report GIT-GVU-14-01*, https://smartech.gatech.edu/bitstream/handle/1853/52020/plsc2014-IoD.pdf?sequence=1 [https://perma.cc/89KH-6NGB] (discussing a refrigerator that will order milk for you when you run out).

29 *A Sea of Sensors*, THE ECONOMIST, IT'S A SMALL WORLD: A SPECIAL REPORT ON SMART SYSTEMS, Nov. 6, 2010, at 6, 6 ("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.").

A. The Internet of Things

The conceptual vision of the Internet of Things promises a world of interconnected smart devices constantly sharing data.[30] As Jeremy Rifkin has written,

> 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.[31]

While such a world of "readable, recognizable, locatable, addressable, and controllable"[32] objects remains in the future, the capacity and interest in tracking everything from our footsteps to our energy usage has spurred exponential growth in developing the "Internet of Everything."[33]

---

30 Quentin Hardy, *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."); PAUL KOMINERS, INTEROPERABILITY CASE STUDY, INTERNET OF THINGS (IOT), The Berkman Center for Internet & Society Research (April 2012), http://cyber.law.harvard.edu/publications ("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.").

31 JEREMY RIFKIN, THE ZERO MARGINAL COST SOCIETY: THE INTERNET OF THINGS, THE COLLABORATIVE COMMONS, AND THE ECLIPSE OF CAPITALISM 11 (2014); *see also* DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS 5–7 (2014) (describing the author's fascination with real and fictional objects "dedicated to a single task of information delivery").

32 Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self* 2.0, 1 J. Sensor & Actuator Networks 217, 217–18 (2012) ("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." (quoting NAT'L INTELLIGENCE COUNCIL, DISRUPTIVE CIVIL TECHNOLOGIES: SIX TECHNOLOGIES WITH POTENTIAL IMPACTS ON US INTERESTS OUT TO 2025 app. F-1 (2008))).

33 *See* DAVE EVANS, THE INTERNET OF EVERYTHING 1 (2012), https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf; Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1, ¶ 10 (2015) ("This so-called Internet of Things—or machine-to-machine connectivity and communications—promises to usher in 'a third computing revolution' and bring about profound changes that will rival the first wave of Internet innovation." (quoting Lee, *supra* note 10 (footnotes omitted))); *see generally* Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 211–12 (2014) (discussing the amount of health information available

As new efficiencies have pushed down the cost of sensors and new innovations have improved the communication capacities of low-power devices, the growth of these smart devices has dramatically expanded.[34] Financial analysts report that the Internet of Things will be a multi-trillion dollar industry involving billions of smart devices.[35] While these numbers mix industrial use with consumer adoption, the promise of tiny, precise, and continuous communicating sensors in localized settings is very real.[36]

The backbone of the Internet of Things involves low-cost, low-power sensors that relay information about smart objects to collecting systems. Early adoption centered on Radio-Frequency Identification (RFID)[37] tags which allowed objects to be marked with unique identifiers and tracked in real time.[38] Development of wireless (Wi-Fi) systems, Bluetooth, and Global

---

to data brokers); Rutledge et al., *supra* note 28 (arguing that the "Internet of Things" is better conceptualized as an "Internet of Devices").

34 Thierer, *supra* note 33, ¶ 12 ("IoT is sometimes understood as being synonymous with 'smart' systems: smart homes, smart buildings, smart appliances, smart health, smart mobility, smart cities, and so on." (footnotes omitted)).

35 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/ [https://perma.cc/T5PD-B9E4]; Swan, *supra* note 32, at 218 ("Cisco estimates that by 2020 there will be 50 billion connected devices, 7 times the world's population.").

36 Steve Lohr, *For Industry, Digital Disruption*, N.Y. TIMES, Nov. 24, 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.").

37 Kyle Sommer, *Riding the Wave: The Uncertain Future of RFID Legislation*, 35 J. LEGIS. 48, 49–51 (2009) ("The RFID tag consists of radio antenna attached to a microchip. These microchips have the capacity to store a variety of information, including item-specific Electronic Product Code (EPC) identifiers, information about the item itself including consumption status or product freshness, or personal identification such as a bank account or social security number."); Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2330 (2007) ("An RFID chip contains a small amount of memory and a wireless antenna. In the presence of a nearby reader device, it functions as a remote bar code. Unlike conventional bar codes, RFID 'tags' need only be in the vicinity of a reader device, not passed manually under a scanner, and they have substantially greater information capacity.").

38 Luigi Atzori et al., *The Internet of Things: A Survey*, 54 COMPUTER NETWORKS 2787, 2788–90 (2010) ("[RFID] [t]ags 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

Positioning Systems (GPS) technologies has allowed for alternative tracking and communication mechanisms.[39] Embedded in physical objects and occasionally people, smart sensors communicate particularized data—"movement, heat, pressure, or location"—about the thing tagged.[40] More sophisticated smart devices such as smartphones essentially provide a cluster of sensor and communications systems that utilize all of the available technologies.[41]

In the consumer space,[42] smart devices have added value and marketing allure to ordinary products. One can now buy a smart watch,[43] drive a smart car,[44] live in a smart home,[45] and even drink from a smart cup that monitors the amount and

---

the need of being in line-of-sight; this allows for mapping the *real world* into the *virtual world*.").

39 Thierer, *supra* note 33, ¶ 11 ("[L]ow-power devices typically rely on sensor technologies as well as existing wireless networking systems and protocols (Wi-Fi, Bluetooth, near field communication, and GPS) . . . ."); Atzori et al., *supra* note 38, at 2787 ("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.").

40 Peppet, *supra* note 5, at 98 ("Microelectromechanical systems (MEMS) sensors translate physical phenomenon, such as movement, heat, pressure, or location, into digital information."); Jones, *supra* note 1, at 41–42 ("In the smart public, things connect regardless of the time, place, path, network, or service. In order for this to occur, physical objects must contain embedded technology to sense and communicate. As wireless protocols become more efficient and sensors and processors become smaller and less expensive, anything can become smart.").

41 *See, e.g.*, Maureen K. Ohlhausen, Commissioner, FTC, Remarks at the Consumer Electronics Show: Promoting an Internet of Inclusion: More Things AND More People 2 (Jan. 8, 2014), https://www.ftc.gov/sites/default/files/documents/public_statements/promoting-internet-inclusion-more-things-more-people/140107ces-iot.pdf [https://perma.cc/8NL4-6FAL] ("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.").

42 For a history of the development of the Internet of Things, including the consumer space, see Ferguson, *supra* note 20, at 812–18.

43 Christopher Mims, *Almost Every Major Consumer Electronics Manufacturer Is Now Working on a Smart Watch*, QUARTZ (July 5, 2013), http://qz.com/101058/smart-watch-explosion/ [https://perma.cc/U43W-YLG8].

44 Henderson, *supra* note 9, at 705 (describing Ford Motor Company's boast of being able to track the driving habits of purchasers through data systems built within the car).

45 Caleb Garling, *Google Enters Homes with Purchase of Nest*, S.F. CHRONICLE (Jan. 14, 2014) ("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 also* NEST, https://nest.com/ [https://perma.cc/DWT2-UVRH] (displaying various smart home technology options).

type of liquids you drink.[46] Wearable technology[47] has revolutionized professional sports,[48] personal fitness training,[49] health monitoring,[50] and has even been incorporated into maternity clothing to track fetal health.[51] A culture of self-monitoring products under the concept of "the Quantified Self"[52] has encouraged cultural acceptance and spurred technological innovation.[53] Future products will include smart heart

---

46 Ellis Hamburger, *Vessyl is the Smart Cup that Knows Exactly What You're Drinking*, THE VERGE (June 12, 2014, 12:00 PM), http://www.theverge.com/2014/6/12/5801106/vessyl-smart-cup-that-knows-exactly-what-youre-drinking [https://perma.cc/5LBN-HPJQ].

47 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 [https://perma.cc/G4Q9-AJDU].

48 Shira Springer, *Sports Wearables Are the Wave of the Future*, BOS. GLOBE (May 25, 2014), http://www.bostonglobe.com/sports/2014/05/24/sports-wearables-are-wave-future/4gwNDNBYxPCEkD4h9yYf8K/story.html [https://perma.cc/D3C3-5PLH]; Kevin Seifert, *Inside Slant: The Other Side of NFL Wearable Technology*, ESPN, (Mar. 2, 2015), http://espn.go.com/blog/nflnation/post/_/id/162679/inside-slant-the-other-side-of-nfl-wearable-technology [https://perma.cc/GUT8-8QH5].

49 Ginia Bellafante, *At the Gym, Abs and Stats*, N.Y. TIMES (Jan. 1, 2016), http://www.nytimes.com/2016/01/03/nyregion/orangetheory-workout-new-years-resolution-fitness.html?_r=0 [https://perma.cc/SCD7-FLDF] (discussing the rise of Orangetheory training, which incorporates wearable devices to record and display fitness progress in real time).

50 Jones, *supra* note 1, at 643 ("Smart socks, made by Heapsylon are infused with textile pressure sensors paired with a set of proprietary electronics that not only accurately track steps, speed, calories, altitude gain, environmental temperature, and distance, but also track cadence, foot landing technique, center of balance, and weight distribution on the foot to help prevent foot injuries for the large niche market of twenty-five million American runners."); Thierer, *supra* note 33, ¶ 22 ("As they grow more sophisticated, wearable health devices will help users track, and even diagnose various conditions, and potentially advise a course of action or, more simply, remind users to take medications or contact medical professionals as necessary. In the process, these health and fitness devices and applications could eventually become 'lifestyle remotes' that help consumers control or automate many other systems around them, regardless of whether they are in their homes, offices, cars, or the like." (footnotes omitted)); Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance [https://perma.cc/LGM9-DNNH].

51 Olivia Lutwak, *Student Creates Smart Maternity Wear*, CORNELL DAILY SUN, Jan. 25, 2015, at 1.

52 *See generally* Swan, *supra* note 32.

53 *See, e.g.*, *Woven Electronics: An Uncommon Thread*, THE ECONOMIST (Mar. 8, 2014), http://www.economist.com/news/technology-quarterly/21598328-conductive-fibres-lighter-aircraft-electric-knickers-flexible-filaments [https://perma.cc/DRY8-GFTM] ("Developments in the use of conductive fibres mean fabric itself can now become an electronic device, allowing wearables to be incorporated into the most stylish clothing."); Finch & Tene, *supra* note 10, 1600 ("Bioaware and wearable devices—already available from t-shirts to smart watches, fitness bands to game consoles—track and interpret even more specific and sensitive human data, such as an individual's heartbeats, eye movements, and gait.").

monitors,[54] smart bandages,[55] and other biological implants.[56] Powerful technology companies such as Apple,[57] Google,[58] and Microsoft[59] are investing in the Internet of Things, not simply to sell products, but to collect the even more valuable data that comes from monitoring those products.[60]

Data—the digital trails of a tracked life—has become a valuable commodity. As Professor Scott Peppet has written, "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."[61] For companies interested in selling products to us, this targeted insight might provide a creepy[62] but relatively benign competitive advantage, but when government and law enforcement have access to

---

54 Thierer, *supra* note 33, ¶ 32 ("CardioMEMS HF System uses a wireless sensor, implanted in the pulmonary artery, to transmit health information to an external device, and 'then [it] forwards the data to the patient's medical team.'" (quoting Maria K. Rega, *Implantable Med Devices: 3 Smart Technologies to Watch*, PTC (June 2, 2014), http://blogs.ptc.com/2014/06/02/implantable-med-devices-3-smart-technologies-to-watch/)).

55 Springer, *supra* note 48 (describing the Biostamp patch).

56 Keiron Monks, *Forget Wearable Tech, Embeddable Implants Are Already Here*, CNN (Apr. 9, 2014, 1:08 PM), http://www.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/ [https://perma.cc/PM4C-PGT7].

57 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 [https://perma.cc/867A-5T6J].

58 Ben Gilbert, *Google Fit Is Android's Answer to Exercise and Health Tracking*, ENGADGET (June 25, 2014, 2:30 PM), http://www.engadget.com/2014/06/25/google-fit [https://perma.cc/G2VQ-FKRN]; Hayley Tsukayama, *Google Develops Android for Wearables You May Actually Want to Wear*, WASH. POST (Mar. 18, 2014, 11:13 AM), http:// www.washingtonpost.com/blogs/the-switch/wp/2014/03/18/google-develops-android-for-wearables-you-may-actually-want-to-wear [https://perma.cc/K3R5-G8QJ].

59 Daniel B. Kline, *How Microsoft Will Incorporate the Internet of Things into Windows 8.1*, MOTLEY FOOL (May 20, 2014, 11:13 AM), http:// www.fool.com/investing/general/2014/05/20/how-microsoft-will-incorporate-the-internet-of-thi.aspx [https://perma.cc/ES39-Z8R9].

60 Wasik, *supra* note 47.

61 Peppet, *supra* note 5, at 90; *see also* Steve Johnson, *Internet of Things Will Transform Life, but Experts Fear for Privacy and Personal Data*, MERCURY NEWS (Nov. 1, 2014), www.mercurynews.com/2014/11/01/internet-of-things-will-transform-life-but-experts-fear-for-privacy-and-personal-data/ ("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.").

62 Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 66–69 (2013).

these data trails, this widening collection of sensors creates significant surveillance concerns.

B. "Sensorveillance"

This Article focuses on what I term "sensorveillance"—here defined as the growth of sensor surveillance to collect and track data among the Internet of Things.[63] The flip side of wonderfully revealing data trails for consumer insights is that those same digital fingerprints can also be used for government investigation.[64] Police entrusted to prevent crime have recognized the value of digital surveillance.[65] As the Internet of Things grows, the data trails from these smart devices will become increasingly helpful to law enforcement.[66]

The reasons for this law enforcement interest are simple and non-technological. Most violent and property crime involves a physical location and a particular time.[67] Geolocational targeting technology can identify suspects near the crime

---

63 The growth of sensor surveillance involves technologies beyond smart devices. As I have written about previously, sophisticated technologies now allow law enforcement to track human movements through facial recognition technology, license plates through automated license plate readers, and old-fashioned video surveillance. The capabilities to track in real-time and over larger areas of a city have been improved by more integrated systems and over-flight capacities. Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1293 (2014); *see also* Richards, *supra* note 6, at 1936 ("The scope and variety of the types of surveillance that are possible today are unprecedented in human history. This fact alone should give us pause."); 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, 1377 (2004) (describing Orwellian surveillance); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 214–15 (2002) ("The advent of sophisticated technology that allows the government to watch, zoom in on, track, and record the activities of anyone, anywhere in public, twenty-four hours a day, demands regulation.").

64 Finch & Tene, *supra* note 10, at 1601 ("The normalizing of constant data collection and bioaware sensors invites private companies literally under our skin; it also opens the door to new forms of government surveillance.").

65 John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES, Nov. 29, 2008, at BU1, http://www.nytimes.com/2008/11/30/business/30privacy.html [https://perma.cc/NZX4-PTRZ].

66 Thierer, *supra* note 33, at ¶ 160 ("The use of wearable technologies by law enforcement officials—or law enforcement's ability to tap into private data flow from wearable devices—deserves special scrutiny and additional legal protections for the public.").

67 This insight was discovered decades ago by the first environmental criminologists. DEREK J. PAULSEN & MATTHEW B. ROBINSON, CRIME MAPPING AND SPATIAL ASPECTS OF CRIME 154 (2d ed. 2009) (discussing the history and role of environmental criminologists); *see also* Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment: Redrawing "High-Crime Areas"*, 63 HASTINGS L.J. 179, 186 (2011) (same).

scene or undermine an alibi defense.[68] Place and time can be recorded with certainty. Suspects can be virtually tracked. Smartphones with tracking capabilities already have been used to prove links to criminal activities.[69] Stingray devices (IMSM catchers) designed to intercept cell phone communications and track locations have been used to identify suspects.[70] As more sensors become embedded with identifiable information, more opportunities will exist to prove geographic and temporal connections to the crime.

Sensors can also reveal information that inferentially might help law enforcement investigate crime. For example, high energy consumption from smart home sensors can reveal marijuana cultivation.[71] Excessive refills from a smart pill bottle of pain killers might suggest substance abuse. Smart cars record speed and distance, and will literally call the police on you when you leave the scene of a hit and run.[72] Finally, wearable fitness sensors provide health data that is granular enough to suggest the use of illegal substances or the type of physical exertion consistent with violent acts.[73] In a case involving drug use, an elevated heartbeat could be used as evidence to prove the time when drugs were ingested.[74] In a case involving an arson suspect, the extent of healing for a burn wound could reveal the time of the arson.[75]

---

68 Derek McAuley, *Century-Old Snooping*, SLATE (Aug. 7, 2014, 7:57 AM), http://www.slate.com/articles/technology/future_tense/2014/08/what_wwi_code_breakers_and_hedy_vlamarr_have_to_do_with_the_internet_of_things.html [https://perma.cc/KAP7-ATUT] ("[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.").

69 Heath Hardman, *The Brave New World of Cell-Site Simulators*, 8 ALB. GOV'T L. REV. 1, 8–10 (2015) (describing use in criminal context); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ [https://perma.cc/B7UL-PKMT].

70 Heath, *supra* note 69.

71 Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, 6 (2008).

72 Alex Hern, *Florida Woman Arrested for Hit-and-Run After Her Car Calls Police*, THE GUARDIAN (Dec. 7, 2015), http://www.theguardian.com/technology/2015/dec/07/florida-woman-arrested-hit-and-run-car-calls-police [https://perma.cc/MH8U-LF7Z].

73 *See* Peppet, *supra* note 5, at 101–02.

74 *See* Ferguson, *supra* note 20, at 820 (describing how an elevated heartbeat can be detected through health monitors).

75 James Gerber, *Flexible Smart Sensors and the Future of Health*, ENGADGET (Sept. 21, 2015), http://www.engadget.com/2015/09/21/flexible-smart-sensors-and-the-future-of-health/ [https://perma.cc/QMX3-YQRB].

Sensor patterns, although not incriminating in themselves, might lead police to develop suspicion.[76] Location sensors might suggest a pattern of proximity to a series of burglaries or sexual assaults. Electronic bank transfers might trigger suspicion of money laundering. Gunshots detected by an acoustic sensor can reveal the presence of an illegal weapon.[77] The list goes on and will only become longer as many of our ordinary activities become mediated through data communications and linked to other digital information sources.[78]

Part II of this Article looks at the legal and constitutional gaps concerning this data, but this section examines the technological vulnerabilities of this new sensor-based world. The focus here is on the direct interception of data trails by police, not indirect access through third parties. Because most data trails arising from the Internet of Things can also be obtained via the third party provider (usually the private company collecting the data), this focus is necessarily limited.[79] However, as has been seen with GPS tracking, Stingrays, and other Wi-Fi

---

76 Peppet, *supra* note 5, at 120 ("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.").

77 Andras Petho et al., *ShotSpotter Detection System Documents 39,000 Shooting Incidents in the District*, WASH. POST (Nov. 2, 2013), https://www.washingtonpost.com/investigations/shotspotter-detection-system-documents-39000-shooting-incidents-in-the-district/2013/11/02/055f8e9c-2ab1-11e3-8ade-a1f23cda135e_story.html [https://perma.cc/JUL2-89DW].

78 A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1726–27 (2015) ("In the very near future, data collected from real-world sensors will routinely be linked to personal information available online. Real-time photos can rapidly be linked to online data.").

79 *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) ("In the case of a third-party victim, the victim's independent interest in transferring the relevant information to law enforcement outweighs the disclosing party's privacy interest."); 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) (providing a 50-state overview of Third-Party Doctrine); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) ("The 'third-party doctrine' is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations.").

sniffing cases, these types of direct police interceptions do occur and need to be explored.[80]

Paralleling the scope of technology, the scope of security of the Internet of Things ranges from the simplistic to the sophisticated. Due to its low cost and limited power and memory, RFID surveillance has been recognized as quite vulnerable to interception.[81] Robust security measures have not been a priority.[82] The lack of security largely has been seen as the cost of ubiquitous connectivity. Even so, the result is that these sensors can be tracked at a distance and without the suspect knowing that they are being so tracked.[83]

Even more sophisticated systems within the Internet of Things reveal concerns with security.[84] Wi-Fi systems have

---

80 *See* United States v. Jones, 132 S. Ct. 945 (2012) (involving usage of GPS data as evidence); Heath, *supra* note 69 (describing the Stingray); Wagenseil, *infra* note 85 (describing devices that use Wi-Fi).

81 Nicole A. Ozer, *Rights "Chipped" Away: RFID and Identification Documents*, 2008 STAN. TECH. L. REV. 1, 7–8 (2008) (discussing the security risks of RFID technology); Sommer, *supra* note 37, at 57 ("Privacy experts have identified three technical aspects of RIFD [sic] tags that generate privacy concerns: they are promiscuous since they will talk to any compatible reader; they are remotely readable since they can read at a distance through obtuse materials like cardboard, cloth, and plastic; and they are stealthy in that the tags are not only inconspicuous, but an individual remains unaware when and to whom the tags are transmitting information or when an unwanted third party is receipting tag information.").

82 Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the 'Security of Things'* 14, 16 (Kelley Sch. of Bus. Res. Paper, Paper No. 16–6), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715799 [https://perma.cc/Y8ZN-RJ6N]; Tom Brewster, *There are Real and Present Dangers Around the Internet of Things*, THE GUARDIAN (Mar. 20, 2014, 9:00 AM), http://www.theguardian.com/technology/2014/mar/20/internet-of-things-security-dangers [https://perma.cc/7ZVH-W9LT]; Nicole Perloth, *Smart City Technology May Be Vulnerable to Hackers,* N.Y. TIMES (Apr. 21, 2015, 1:59 PM), http://bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers/ [https://perma.cc/3QWE-QNQR].

83 Sommer, *supra* note 37, at 50 ("Unlike other Auto-IDs such as bar codes, RFID is a relatively small, fast, technology 'that enables tracking and monitoring activities to be carried out using invisible radio waves over distances that range from less than a centimet[er] to many hundreds of met[er]s.'") (quoting ALAN BUTTERS, RADIO FREQUENCY IDENTIFICATION: AN INTRODUCTION FOR LIBRARY PROFESSIONALS 2 (2006), http://www.sybis.com.au/sybis/RFID%20Whitepaper.pdf.).

84 Kashmir Hill, *The Half-Baked Security of Our 'Internet of Things,'* FORBES (May 27, 2014, 2:56 PM), http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things [https://perma.cc/XG6D-4MJX]; John Brandon, *Wearable Devices Pose Threats to Privacy and Security*, FOX NEWS (June 18, 2014), http://www.foxnews.com/tech/2014/06/18/wearable-devices-pose-threats-to-privacy-and-security [https://perma.cc/W4RJ-E363]; *Home, Hacked Home: The Perils of Connected Devices*, THE ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home [https://perma.cc/A3Y6-2LRE].

been intercepted with relative ease.[85] Bluetooth technologies have shown hacking vulnerabilities.[86] Cell phones, while protective of communication content, have had their location data revealed by Stingray devices.[87] Wearables have been subject to snooping.[88] Home sensors have revealed lifestyle and appliance use information.[89] Even smart cars have been taken over by hackers wishing to demonstrate security concerns.[90]

---

85 Paul Wagenseil, *Google Spy Case Shows Why You Should Encrypt Your Wi-Fi*, NBC NEWS (May 1, 2012, 9:19 AM), http://www.nbcnews.com/technology/technolog/google-spy-case-shows-why-you-need-encrypt-your-wi-744411 [https://perma.cc/R4F4-9JNB] ("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.").

86 Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, 44 (2008) ("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. 2004), http://www.wired.com/wired/archive/12.12/phreakers_pr.html (describing Bluetooth attacks on cellphones)).

87 Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 11 (2014).

88 *BitDefender Finds Phone to Smart Watch Communications Easy to Snoop*, THE SECURITY LEDGER, https://securityledger.com/2014/12/bitdefender-finds-phone-to-smart-watch-communications-easy-to-snoop/#.VIsbz3uaWDk [https://perma.cc/A2TJ-U55L] ("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 5, at 134 ("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]).

89 2 NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBERSECURITY 25 (2014), http:// nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf [https://perma.cc/GG45-VEAH] (demonstrating how smart meter data reveals lifestyle and appliance use information); Jordan Robertson, *Your Outlet Knows: How Smart Meters Reveal Behavior at Home, What We Watch on TV*, BLOOMBERG (June 11, 2014), http://www.bloomberg.com/news/2014-06-10/your-outlet-knows-how-smart-meters-can-reveal-behavior-at-home-what-we-watch-on-tv.html [https://perma.cc/C4HH-QJRD].

90 *See* Larry Greenemeier, *Fact or Fiction?: Your Car Is Hackable*, SCI. AM. (Apr. 2, 2014) http://www.scientificamerican.com/article/fact-or-fiction-your-car-is-hackable1 [https://perma.cc/69CW-V7DR]; Keith Barry, *Can Your Car Be Hacked?*, CAR & DRIVER (July 2011), http://www.caranddriver.com/features/can-your-car-be-hacked-feature [https://perma.cc/9VN6-L459]; *cf.* Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driv-*

While smartphone companies have responded with increased encryption,[91] and a movement has grown to combat concerns about government surveillance,[92] the Internet of Things remains relatively unprotected.[93] These current security concerns become exacerbated when one considers problems of interconnectivity and obsolescence.[94] First, part of the value of smart devices is being able to use other sources of information to improve efficiency and convenience. Perhaps your home heating system is dependent on the weather forecast, which means the device is also dependent on the security of the weather forecasting service. Any weak link in any data provider can compromise the security of the entire system.[95] Or perhaps your system is completely secure now, but in five years (a lifetime for digital devices) the system needs an upgrade and the security upgrade is not compatible with the old system. Robust security requires regular updating (patching of security holes), and most smart devices do not have that capability, not to mention that most consumers do not have the interest in constantly purchasing new smart devices to keep up with security vulnerabilities.[96] Unlike a smartphone, which you might regularly exchange every few years, you will not be purchasing a new smart refrigerator at the same pace.

Smart devices and the data communicated by them provide a new frontier in the world of surveillance.[97] Technological fixes and hacks will continue apace. Government agents will

---

erless Cars, 5 WAKE FOREST J.L. & POL'Y 339, 376 (2015) (noting that it may already be possible to hack cars that have automatic cruise control).

91 Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html [https://perma.cc/Z2AK-GBCP].

92 *See generally* Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 999–1002 (2013) (discussing various ways people have protested government surveillance).

93 FED. TRADE COMM'N, THE 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/CK57-ULNL].

94 *See The Internet of Unpatched Things*, presentation by Sarthak Grover and Nick Feamster at the FTC PrivacyCon Conference (Jan. 14, 2016), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf [https://perma.cc/3T96-FAHK] (detailing the risks associated with "unpatched" internet devices).

95 *See id.*

96 *See id.*

97 *Don't Panic: Making Progress on the Going Dark Debate*, THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/XP7S-K7SW] ("The audio and video sen-

see the value of these advancements for crime suppression and investigation. The question will be how the law adapts to this changing field. The constitutional question is the subject of Part II.

II
THE FOURTH AMENDMENT AND DATA TRAILS

This section examines how the Fourth Amendment might address the surveillance of smart objects. Data and data trails obviously were not considered by the drafters of the Fourth Amendment.[98] Yet, the Fourth Amendment's protection has expanded beyond the pre-electronic, pre-digital world of the Founding.[99] The Supreme Court has regularly addressed technological innovations, expanding the definitions and protections of Fourth Amendment rights in the face of inventions such as automobiles, telephones, and tracking devices.[100]

Fourth Amendment doctrine is anything but clear, as conflicting theories of constitutional interpretation and ever-widening exceptions have resulted in a confused patchwork of protections.[101] Unraveling the various doctrinal threads reveals a knotty, tangled, but growing web of Fourth Amendment rules and principles, none of which obviously apply to data trails. Yet, examining the question of data trails does reveal a unifying principle that suggests a way forward. Underlying the protection of most persons, homes, papers, effects, and expectations of privacy is a concern for personal information—information that allows for self-expression, autonomy, association, religion, liberty, family, and security.[102] As will be

---

sors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications.").

98 The Fourth Amendment was ratified in 1791 before the advent of electricity or computers. One of the earliest articulations of the world of smart devices can be found two hundred years later in 1991, in Mark Weiser's Scientific American article "The Computer for the 21st Century." *See* Mark Weiser, *The Computer for the 21st Century*, SCI. AM. (Sept. 1991), https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf [https://perma.cc/4RTF-WFWT].

99 *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2477 (2014) (smartphones); Kyllo v. United States, 533 U.S. 27, 34–37 (2001) (thermal imagers); United States v. Karo, 468 U.S. 705, 716 (1984) (beepers); Katz v. United States, 389 U.S. 347, 351–52 (1967) (telephones).

100 Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 405 (2013); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011).

101 *See* Ferguson, *supra* note 63, at 1293 (describing the Fourth Amendment as a "doctrinal muddle").

102 This insight has been previously recognized by privacy law scholars and criminal justice scholars. *See, e.g.*, Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 583 (1990) ("If the fourth

discussed, the study of data trails brings into stark relief the Fourth Amendment's long-standing concern for informational security.[103]

The first part of this section briefly summarizes the existing state of Fourth Amendment doctrine, highlighting suggestions from recent cases about how digital information might be covered. The second part explores how the Fourth Amendment maps onto the puzzle of data trails, revealing a significant gap in constitutional protections.

A. Existing Fourth Amendment Framework

The Fourth Amendment protects against unreasonable searches and seizures.[104] Arising from the Founders' concern with arbitrary government surveillance,[105] the Fourth Amendment establishes constitutional limits on police power.[106] Like

---

amendment was intended to promote a sense of personal security, it must extend to the protection of informational privacy."); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1021 (1995) ("[I]nformational privacy—privacy as nondisclosure—is and has been preeminent. . . . The question, in other words, is whether what the police did was likely to capture something secret." (emphasis omitted)); Tomkovicz, *supra* note 22, at 665–66 ("Recognition of the fundamentally information-acquisitive nature of constitutional searches leads logically toward a conception of the fourth amendment's ward as primarily informational privacy—that is, an interest in maintaining confidentiality or secrecy, in not having data about one's life learned by the government."); *but see* Louis Michael Seidman, *The Problems with Privacy's Problem*, 93 MICH. L. REV. 1079, 1086 (1995) (arguing that modern Fourth Amendment law is not about privacy, but limiting the "collateral damage" from searches and seizures); Louis Michael Seidman, *Making the Best of Fourth Amendment Law: A Comment on* The Distribution of Fourth Amendment Privacy, 67 GEO. WASH. L. REV. 1296, 1301 (1999) ("The Fourth Amendment is not solely about informational privacy. It also speaks to humiliation, inconvenience, embarrassment, and violence.").

103 As will be discussed in Part III, informational security is distinguished from privacy. While certain definitions of privacy might perfectly overlap with a concept of intentionally excluding others from one's personal sphere of influence, see ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967), the Supreme Court's conception of privacy—influenced by the false friend doctrine, the third party doctrine, and the *Katz* progeny does not so overlap. Thus, as a constitutional matter there exists a need to redefine this secure informational space.

104 *See* U.S. CONST. amend. IV.

105 *See* United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) (explaining that the purpose of the Fourth Amendment is to protect against "arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals" (citations omitted)); Dow Chem. Co. v. United States, 476 U.S. 227, 240 (1986) (Powell, J., dissenting) ("The Fourth Amendment protects private citizens from arbitrary surveillance by their Government.").

106 Riley v. California, 134 S. Ct. 2473, 2494 (2014) ("Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for

many provisions in the United States Constitution, the meaning of those limits has been regularly debated in scholarly commentary.[107] Many engaging histories of the Fourth Amendment exist,[108] and many more theories about how to understand the doctrine have been generated.[109] For purposes of this Article, a brief overview suffices to set the stage for later analysis.

For the Fourth Amendment to apply, government agents must conduct a "search" or "seizure."[110] Searches and seizures are terms of art in the Fourth Amendment and have been defined variously in different eras.[111] After a quiet beginning with essentially no major Fourth Amendment cases for 100 years,[112] the Supreme Court decided *Boyd v. United States*,[113] a case involving a court order demanding that a commercial glass company produce private business papers.[114] Relying on the Fourth and Fifth Amendments, the Court held that such a

---

evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.").

107 *See generally* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757–61 (1994) (referring to modern Fourth Amendment jurisprudence as "an embarrassment" and a "mess"); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 353–54 (1974) (identifying and discussing a number of issues that complicate the development of a single Fourth Amendment theory); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 556 (1999) (arguing that search and seizure doctrine has evolved and provided officers with "far more discretionary authority than the Framers ever intended or expected"); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 823 (1994) (disagreeing with scholars who look to the intent or expectations of the Framers to shape Fourth Amendment law).

108 *E.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES (1997); THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION (2008); WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791 (2009) (publishing William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* (1990); ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789–1868 (2006).

109 *E.g.*, Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 308 (1998); Davies, *supra* note 107, at 550; Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 562 (1996); Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 960–65 (1997); David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1741 (2000); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 415 (1995).

110 *See* U.S. CONST. amend. IV.

111 *See infra* Part II.

112 Boyd v. United States, 116 U.S. 616 (1886).

113 *Id.*

114 The business was E.A. Boyd and Sons. *See id.* at 616–19.

demand violated the Constitution.[115] The Court focused on the informational harm in being compelled to reveal private information through governmental coercion:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employ[ee]s of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence . . . .[116]

Three points about *Boyd* are notable for an article focused on informational security. First, in referencing "the privacies of life" the Court appeared to focus on harm independent of the physical invasion of "breaking of his doors" or "rummaging of his drawers."[117] At issue in *Boyd* was a formal court order requesting papers through a court process. The harm involved revealing information, not forceful, physical searching or seizing. Second, the focus was obviously on the information in the papers, not the physical parchment itself. "Papers" has been the proxy term for protecting the contents in the papers, not merely the existence of the papers. Third, the context of the case—involving business records, as opposed to, for example, a personal diary, suggests that the reach of these privacies of life goes beyond revealing personal information and covers privately held, but not overtly intimate, information.[118]

As students of the Fourth Amendment know, this broad protection in *Boyd* was soon replaced with a more limited, physically-oriented, property-based understanding of a search focused on the textual language of "persons, houses, papers, and effects."[119] From *Boyd* to the 1960s, the Supreme Court

---

115 *Id.* at 622 ("It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution, in all cases in which a search and seizure would be; because it is a material ingredient, and effects the sole object and purpose of search and seizure.").

116 *Id.* at 630.

117 *Id.*

118 *Boyd* had a brief Fourth Amendment impact, in part because it was seen as more of a Fifth Amendment case. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 814 (2005).

119 Jack Wade Nowlin, *The Warren Court's House Built on Sand: From Security in Persons, Houses, Papers, and Effects to Mere Reasonableness in Fourth Amend-*

generally looked to see if persons, papers, homes, or effects were physically invaded, triggering the protection of the Fourth Amendment.[120] This so-called trespass doctrine[121] created some anomalous rulings, so, for example, a microphone placed on a wall to eavesdrop on an adjoining room would not be considered a search because no physical intrusion of a protected space occurred,[122] but a "spike mike" that barely pierced the adjoining wall to capture the same conversation would have been a search (because of the minimal trespassory intrusion).[123] Such reasoning was criticized as being too limiting and ignoring the technological developments that could soon invade privacy without physically intruding on constitutionally protected spaces.[124]

In response, the Supreme Court began to develop the now familiar "reasonable expectation of privacy" theory in *Katz v. United States*.[125] Justice Harlan established the new test in a concurrence, asking whether an individual has a subjective expectation of privacy that society deems objectively reasonable.[126] In *Katz*, the issue was whether the conversation of

---

ment Doctrine, 81 MISS. L.J. 1017, 1031–32 (2012) ("This traditional [protected interest] 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." (citations omitted)). *But see* Orin Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 68 (2012) (arguing that the Court did not use a specific formulation to identify what counted as a Fourth Amendment search).

120 Kyllo v. United States, 533 U.S. 27, 31 (2001) ("[W]ell into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." (citations omitted)); 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) ("Until the 1960s, the Fourth Amendment protected against government trespass in any of the four areas named in the Fourth Amendment—houses, persons, papers, and effects. Under that approach, the prevalence of technology the police used was irrelevant. The sole inquiry was whether operation of the technology required intrusion into a protected area. If so, a search occurred; if not, then the Fourth Amendment was not implicated." (citations omitted)).

121 Kerr, *supra* note 119 (arguing that the so-called trespass doctrine did not in fact control early Fourth Amendment cases).

122 *See* Goldman v. United States, 316 U.S. 129, 135 (1942).

123 Silverman v. United States, 365 U.S. 505, 509–12 (1961).

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

125 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 996 (2008) ("*Katz* signified a shift away from the property-trespass theory of Fourth Amendment analysis by finding a constitutionally protected interest separate from any place and distinct from tangible property.").

126 *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement,

Charlie Katz with his gambling associates picked up by a microphone taped to a public telephone booth was a search.[127] No physical invasion of the phone booth occurred, but the Court majority reframed the issue by explaining that the Fourth Amendment protected "people, not places."[128] Justice Harlan's concurrence completed this reframing with its reasoning that, by shutting the door and paying his "toll" to use the payphone, Katz could claim a "reasonable expectation of privacy" in the content of his call.[129]

Since *Katz*, the reasonable expectation of privacy test has controlled the threshold analysis of whether a Fourth Amendment search has occurred. The test, however, has also created some counter-intuitive results. For example, the Supreme Court has held that use of a low-flying plane to look into a suspect's backyard is not a "search" because such an action did not violate a reasonable expectation of privacy.[130] Clearly, police were "searching" in the ordinary sense of the term, looking for incriminating information, but it was not a Fourth Amendment search because no expectation of privacy had been violated.[131] Significant scholarly effort has been expended to define whether a reasonable expectation of privacy exists in an object, or area, or thing.[132] Despite criticism and debate, the reasonable expectation of privacy test has since been cited tens of thousands of times and rather singularly controlled Fourth

---

first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

127 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 820 (2004).

128 *Katz*, 389 U.S. at 351 (majority opinion); *id.* at 361 (Harlan, J., concurring).

129 *Id.* at 360–61 (Harlan, J., concurring) ("The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted." (quoting *id.* at 352 (majority opinion))).

130 *See* California v. Ciraolo, 476 U.S. 207, 213–14 (1986).

131 *See id.*

132 *E.g.*, Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1241 (2012); Katz, *supra* note 102, at 505–07; Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314, 315–20 (2012); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505–07 (2007); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1334–36 (2012); 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); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 857–58 (2002); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125 (2002).

Amendment search questions up until 2012 and Justice Antonin Scalia's majority opinion in *Jones v. United States*.[133]

Pre-*Jones*, conventional wisdom held that the trespass theory of the Fourth Amendment had been relegated to history, essentially overruled by *Katz*.[134] However, in a case that involved the warrantless Global Positioning Satellite (GPS) tracking of a suspect's car for twenty-eight days, Justice Scalia reclaimed the trespass theory as a viable Fourth Amendment alternative.[135] Justice Scalia explained that by "physically occupy[ing] private property for the purpose of obtaining information" (placing the GPS on the car), the police conducted a search.[136] The private property was Jones' wife's car (an effect), and the placement of the GPS device with the intent to obtain personal information from the device constituted a search.[137] Justice Scalia reiterated the importance of the term "effect" and its close association with the protection of private property.[138] While conceding the continued viability of the reasonable expectation of privacy theory, Scalia offered an 18th Century solution for a 21th Century problem.[139]

Of note, five Justices concurred in *Jones*, but on different grounds. The concurring Justices found that twenty-eight days of warrantless GPS surveillance for a narcotics investigation should be considered a Fourth Amendment search because it violated a reasonable expectation of privacy.[140] Justice Sonia Sotomayor, who joined the majority opinion but wrote separately, first agreed with Justice Scalia that "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment

---

133 United States v. Jones, 132 S. Ct. 945, 947 (2012).

134 As mentioned *supra*, some scholars have since pointed out that there may never have been an actual trespass theory. *See* Kerr, *supra* note 119 and explanatory parenthetical at *supra* note 121.

135 *See Jones*, 132 S. Ct. at 949–52.

136 *Id.* at 949.

137 *See id.*

138 *Id.* ("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.").

139 *Id.* at 953 ("Unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."); *see id.* at 957–58 (Alito, J., concurring) (criticizing the majority's reliance on 18th Century tort principles).

140 *See id.* at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

protection."[141] But, Justice Sotomayor went on to note that a broader protection may also be needed when facing advanced surveillance techniques, "[w]ith increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones."[142] To combat these technological threats to privacy and security, Justice Sotomayor reframed the Fourth Amendment question, stating: "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."[143]

Justice Samuel Alito, writing for four Justices, also relied upon a reasonable expectation of privacy test to determine whether the GPS surveillance constituted a Fourth Amendment search.[144] After roundly criticizing the majority for adopting an outdated Fourth Amendment theory, Justice Alito concluded that long-term GPS surveillance for most offenses would be a Fourth Amendment search. However, Justice Alito left unanswered exactly how to define "long-term" and "most offenses."[145]

The result—post-*Jones*—is that courts facing Fourth Amendment questions about locational data or other information must analyze both the reclaimed physical intrusion theory and the reasonable expectation of privacy theory to determine if a Fourth Amendment search has occurred. Neither theory has been fully developed to reflect the digital world, and the Court's most recent Fourth Amendment and technology case, *Riley v. California*,[146] only adds to the uncertainty.

Riley involved the Court's first attempt to reconcile smartphone data and Fourth Amendment doctrine. The case itself asked whether police need a warrant to search a smartphone incident to arrest.[147] David Leon Riley had been stopped for driving without a license, and guns had been recov-

---

141 *Id.* at 954 (Sotomayor, J., concurring).
142 *Id.* at 955 (Sotomayor, J., concurring).
143 *Id.* at 956 (Sotomayor, J., concurring).
144 *Id.* at 964 (Alito, J., concurring).
145 *Id.* at 964 ("Under this approach, 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." (internal citation omitted)).
146 134 S. Ct. 2473, 2484 (2014).
147 *Id.* at 2480.

ered from his car. Police believed Riley might be involved in gang violence. In scrolling through the data in Riley's smartphone after his arrest, police uncovered an incriminating photograph later used against him in trial. Riley moved to suppress the warrantless search of his smartphone data incident to arrest.

The difficulty for the Court was that blind application of non-digital precedent to a digital problem did not offer much Fourth Amendment protection.[148] In an earlier case, *United States v. Robinson*, the Court had upheld the search of a cigarette pack recovered incident to an arrest.[149] The question was whether searching a smartphone could be considered the equivalent type of invasion, or whether the digital nature of the smartphone changed the analysis. In *Riley*, the Supreme Court reasoned that smartphone data was quantitatively and qualitatively different than searching a cigarette pack or even a wallet or address book recovered from an arrested suspect.[150] In concluding that police did need a warrant before searching the smartphone data, the Court made several statements relevant to how the Fourth Amendment might conceptualize data trails arising from smart objects.

First, the Court explicitly recognized that data distorts traditional application of legal precedent based on physical objects.[151] Data is different because ordinary physical constraints and physical limitations fall away in a digital world.[152] In the context of a smartphone, data storage allows for vastly more information to be collected about an individual.[153] Data aggregation allows for a qualitatively more complete picture of

---

148 *Id.* at 2484 (recognizing that a mechanical application of precedent might result in upholding a warrantless search).

149 414 U.S. 218 (1973).

150 *Riley*, 134 S. Ct. at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person.").

151 *Id.*

152 *Id.* ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

153 *Id.* ("But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on." (internal citations omitted)).

that individual to be drawn.[154] Data sharing means that the information is not stored in one central place, but can live on a device, on a cloud, and in between.[155] Finally, the pervasiveness of digital technology threatens to invade "the privacies of life,"[156] as actions, thoughts, and patterns become reflected in digital form.[157] In borrowing the language from *Boyd*, Chief Justice Roberts brought the informational nature of the Fourth Amendment invasion full circle.[158] Unfortunately, while the Court appeared to recognize that data is different, it did not provide any answer for how the Fourth Amendment should conceptualize data outside of the search incident to arrest context. *Riley* began reimagining a digital Fourth Amendment, but provided only an incomplete picture.

As a final issue, the "third party doctrine" creates an additional problem for the Fourth Amendment.[159] As currently understood, information provided to a third party (e.g., a phone company, friend, or any of the companies providing devices in the Internet of Things) loses protection under a reasonable expectation of privacy theory.[160] The rationale has been that by giving the information to another, the giver loses a claim to

---

154 *Id.* at 2490 ("Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

155 *Id.* at 2491 ("To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter."); *see id.* ("[W]ith increasing frequency, [cell phones] are designed to . . . tak[e] advantage of 'cloud computing.' Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.").

156 *Id.* at 2495 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

157 *Id.* at 2490 ("[T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day.").

158 *Boyd*, 116 U.S. at 630.

159 *See supra* note 79.

160 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006) ("[Third-party] doctrine provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information.").

privacy over the information.[161] Academics have criticized the doctrine as being ill-suited for the digital age.[162] Justice Sotomayor in *Jones* suggested reconsidering it.[163] Despite these criticisms, the practical reality remains that because data is usually held by another entity as well as the owner, a broad reading of the third party doctrine undermines Fourth Amendment protection for most data trails. For purposes of this Article, the focus is on the direct interception of data trails, rather than third party collection. This Article asks whether the Fourth Amendment protects the direct interception, collection, and use of data trails by law enforcement. If the answer is no, then there is no Fourth Amendment protection for the data trails we create. If the answer is yes, then the third party doctrine may still allow a work-around for law enforcement to get the same information indirectly (via the third party). Both problems need to be addressed, but this Article only focuses on the direct collection issue.

As can be seen, difficult questions emerge from applying Fourth Amendment doctrine to this problem of data. How can one trespass or physically intrude on data trails which have no physical being?[164] How does one define a threshold line for a reasonable expectation of privacy test around an intangible, instantaneous, mutable representation of digital code? How should society think about the data arising from the home, effects, person, and papers? These are difficult, theoretical questions that will begin to be considered in the next section.

B. Doctrine and Data Trails

To visualize how traditional Fourth Amendment doctrine might apply in the Internet of Things world, consider the follow-

---

161 *Compare* Kerr, *supra* note 79, at 564 (justifying the rule based on consent and the need for "technological neutrality"), *with* Erin Murphy, *The Case Against the Case for the Third Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1241–46 (2009) (criticizing Kerr and debating whether the doctrine should exist at all).

162 *See, e.g.*, Murphy, *supra* note 161, at 1242 n.11 (arguing that the rule has too broad a reach in a world where "we are all citizens of technology").

163 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

164 *See, e.g.*, 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." (citation omitted)).

ing scenario. Most mornings I wake up and brush my teeth with a smart toothbrush that has the Wi-Fi capability to be connected with a smartphone and beyond.[165] Data about my teeth brushing habits is generated and sent to collecting sensors and receptors. The data reveals something personal about my hygiene habits, reveals a pattern of my waking time and sleeping time, and arises from inside my *person* (my mouth). The data also derives from my bathroom in my *home*. The data comes from my personal *effect* (the toothbrush). The data when translated into a smartphone record or a dentist's office report becomes the equivalent of a *paper* record of brushing, as if I manually wrote down the frequency of my teeth brushing routine in a notebook. In addition, I subjectively expect that my oral hygiene habits will not be intercepted by others, and imagine that such an expectation of privacy is objectively reasonable under a *reasonable expectation of privacy* theory. And, while the analysis changes if I move outside my home, I still expect the same sort of privacy if I should take my toothbrush to work, on a business trip, or even use it on my commute in my car. At the same time, the unencrypted data from my toothbrush could be intercepted by anyone interested in monitoring me. Similarly, any data shared with a third party would be in the hands of third parties and thus, obtainable from those third parties. In short, the data trails created by one of many smart objects in my daily life creates an opportunity to examine how the Fourth Amendment should consider data that is connected to a smart object, but also distinct from that object.

How should the Fourth Amendment treat direct interception of these data trails? Three distinct approaches emerge from the current doctrinal uncertainty. First, one could apply Justice Scalia's physical intrusion/trespass theory announced in *Jones*.[166] Second, one could apply the traditional *Katz* reasonable expectation of privacy test.[167] Third, and relatedly, one could find that such data deserves no reasonable expectation of privacy because such a claim to privacy is objectively unreasonable or because it falls within one of the established exceptions (abandonment, third party doctrine, etc.).[168] As such, the data trails would exist outside of Fourth Amendment protection.

---

165 It was a Father's Day gift. Don't judge.

166 *See* United States v. Jones, 132 S. Ct. 945, 949–52 (2012).

167 *See* Katz v. United States, 389 U.S. 347, 360 (1967).

168 *See* Solove, *supra* note 160; California v. Greenwood, 486 U.S. 35, 39–41 (1987).

This section begins by applying these approaches to data trails arising from effects, homes, persons, and papers. This section examines the Supreme Court's recent focus on constitutionally protected spaces in *United States v. Jones* (effects),[169] *Florida v. Jardines* (homes),[170] and *Grady v. North Carolina* (persons),[171] as well as the traditional reasonable expectation of privacy test, showing that doctrinal gaps exist with both approaches. This section also identifies a unifying theme that demonstrates the Fourth Amendment's longstanding concern with informational security arising from constitutional sources. As will be discussed, the study of data trails reveals an information-based foundation for the Fourth Amendment more appropriate for the digital future.

1. *"Effects" and Data Trails*

The Fourth Amendment protects personal property through the term "effects." In *Jones*, the majority specifically located the constitutional harm of placing the GPS device on the car (the effect), citing to the recognition that the Fourth Amendment protects our personal property from law enforcement interference.[172]

Effects have historically been understood to mean personal property—the objects we possess.[173] The early American understanding distinguished personal property from real property.[174] Personal property meant physical belongings. Real property meant land. Both were obviously prized by the Founders, but the constitutional language only focused on the former.[175] While James Madison's first draft of what would become the Fourth Amendment originally used the broader language "their other property," this language was changed by the drafting committee to "effects."[176] As Professor Thomas

---

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

170 133 S. Ct. 1409, 1414 (2013).

171 135 S. Ct. 1368, 1370 (2015).

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

173 Altman v. City of High Point, N.C., 330 F.3d 194, 201 (4th Cir. 2003) ("'[E]ffects' 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 . . .'); NOAH WEBSTER, FIRST EDITION OF AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE (1828) (defining "effect" as "[i]n the plural, effects are goods; moveables; personal estate").

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

175 *Id.* at n.7.

176 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 COMM. OF ELEVEN REPORT (July 28, 1789), *reprinted*

Davies has written, "[b]ecause '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."[177] Since that time, the Supreme Court has accepted that "[t]he Framers would have understood the term "effects" to be limited to personal, rather than real property."[178]

The Founding generation prized the protection of personal property not simply because it conveyed ownership or material security, but also because these objects protected self-expression, dignity, and personal relationships.[179] In a recent article, Professor Maureen Brady examined the neglected history of effects in the Founding Era.[180] Specifically, she identified the concern surrounding Founding-era searches of clothing—the confiscation of which might interfere with one's status in civilized society (if you did not have the appropriate attire you could not fully participate in civil society).[181] In addition, she discussed the confiscation of family heirlooms that impacted connections to particular cultural traditions, religions, and identities.[182] The inclusion of effects, therefore, was more than about protecting valuable possessions, but also about protect-

---

in THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 223–24 (Neil H. Cogan ed. 1997)).

177 Davies, *supra* note 107, at 710–11.

178 *Oliver*, 466 U.S. at 177 n.7 (citing Doe v. Dring, 2 M. & S. 448, 454, 105 Eng. Rep. 447, 449 (K.B.1814)).

179 Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964) (arguing that privacy protects human dignity and autonomy); Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1277 (2012) ("The history of the Fourth Amendment amply supports the notion that it protects against the humiliation and loss of dignity wrought by unreasonable government searches and seizures."); Tomkovicz, *supra* note 13, 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." (internal footnotes omitted)).

180 Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 Yale L.J. 946, 980–87 (2016).

181 *Id.* at 987–88 (citing *To the Farmers and Planters of Maryland*, MD. J., Apr. 1, 1788, *reprinted in* 5 THE COMPLETE ANTI-FEDERALIST 74, 75 (Herbert J. Storing & Murray Dry eds., 1981) ("Nay, they often search the clothes, petticoats and pockets of ladies or gentlemen (particularly when they are coming from on board an East-India ship), and if they find any the least article that you cannot prove the duty to be paid on, seize it and carry it away with them; who are the very scurf and refuse of mankind, who value not their oaths, and will break them for a shilling.")).

182 *Id.* at 988.

ing the values of what those objects symbolized. It was not just about protecting property but about protecting objects of self-expression.

Effects populate much of the modern Internet of Things with the only difference from the Founding Era being the stored data inside these smart devices and the data trails emanating from them. From smart umbrellas that tell you whether it is going to rain,[183] to smart pill bottles to remind you to take your medicine,[184] ordinary effects have become sources of data and data trails. As one example, technologist and professor David Rose describes his vision for the ambient umbrella:[185]

> The Ambient umbrella has one enchanted feature—to prompt you to take it with you when you head out the door. A wireless receiver in the handle of the umbrella connects to the nationwide Ambient network and receives data from AccuWeather for your zip code. If rain is forecast, a ring of LEDs embedded at the top of the umbrella's handle glows and pulses a gentle blue light.[186]

The umbrella is an effect. Because it relies on local weather forecasts, it generates locational data and, of course, weather forecasts. If police placed a GPS device on the umbrella to track the umbrella, Justice Scalia's analysis in *Jones* would control.[187] Like the car, the physical placement of the device with the intent to obtain information would constitute a search. But, what if the data trails were just collected by an investigating agent that could track and read the geolocational information without physically touching the umbrella. Is intercepting these signals a search of the effect? As will be explained below, neither the physical intrusion test nor the *Katz* test adequately resolve the issue.

a. *Data from Effects: Physical Intrusion/Trespass Test*

Under a narrow reading of *Jones*'s physical intrusion/trespass test, no Fourth Amendment search would occur with the mere interception of data trails from a smart effect. According to Justice Scalia's theory, the triggering of Fourth Amendment protection requires some physical trespass no matter how slight. Justice Scalia foresaw this issue in *Jones*, stating

---

183 ROSE, *supra* note 31, at 7 (defining an enchanted object as "ordinary things made extraordinary").

184 *Id.* at 9 (describing smart umbrellas).

185 *Id.* at 109–10.

186 *Id.* at 109.

187 *See supra* subpart II.A.

"[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[188] Presumably, according to Justice Scalia's *Jones* theory, intercepting data without a physical trespass means there is no Fourth Amendment search of the effect.

b. *Data from Effects: Reasonable Expectation of Privacy Test*

The concurring Justices in *Jones* provided a partial answer to the question of whether data trails from smart effects should be protected under a reasonable expectation of privacy test. A majority of Justices concluded that collecting long-term, aggregated data trails (GPS data) from an effect would constitute a Fourth Amendment search for most crimes.[189] This test helps, but leaves open many questions. For example, if the data trails from the smart umbrella are not aggregated or collected for a long period of time, does the holding still apply? One can easily imagine a scenario in which the next Antoine Jones (carrying his smart umbrella) enters a narcotics stash house only once, and the information sought to be introduced in court centers around that single trip, intercepted as a single point of data. The carefully worded language in the concurrences—emphasizing aggregation and long term tracking—counsels against an automatic finding of a reasonable expectation of privacy.[190] Further, the nature of the data being largely unsecured, and the actions being publicly observable, also cut against a finding of a reasonable expectation of privacy.[191] While in no way settled, there are good reasons to think that a reasonable expectation of privacy test would not automatically or completely protect the data trails from effects connected in the Internet of Things.

The Supreme Court's prior cases involving the reasonable expectation of privacy in effects also fail to provide guidance in analyzing data trails. In part, this may be because the Court has left "effects" relatively under-theorized. In *United States v. Chadwick*, the Supreme Court established that closed containers—as effects—were protected by the Fourth Amendment: "the Fourth Amendment . . . draws no distinctions among 'per-

188 United States v. Jones, 132 S. Ct. 945, 953 (2012).
189 *Id.* at 964. (Alito, J. concurring).
190 *Id.*
191 *See* United States v. Karo, 468 U.S. 705, 708 (1984); *see also* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.").

sons, houses, papers, and effects' in safeguarding against unreasonable searches and seizures."[192] In *Chadwick*, the effect was a closed footlocker, but the court has expanded the protection of effects to parcels, automobiles, luggage, and the various closed containers seized by police.[193]

For closed containers, what has mattered was not what was in the closed effect (usually contraband in criminal cases), nor the possibility that the container could be examined (certainly possible), but instead the fact of concealment:[194]

> 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.[195]

As long as the closed container (effect) was in the possession of the individual and served to conceal the contents from outside view, the Fourth Amendment protects the privacy and security of the concealed object.

These two qualifiers—possession and concealment—serve to limit the Fourth Amendment protection of effects. If one loses possession of an object—voluntarily abandons it—the court has concluded that such relinquishment of control also relinquishes an expectation of privacy in the object. In *California v. Greenwood*, the court held that private trash secured in opaque bags lost any expectation of privacy because the bags had been abandoned.[196] Similarly, the plain view doctrine has allowed police to view and seize contraband—effects—in plain

---

192 United States v. Chadwick, 433 U.S. 1, 8 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

193 *Id.* at 11 ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause.").

194 *Acevedo*, 500 U.S. at 598 (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.").

195 United States v. Ross, 456 U.S. 798, 822 (1982) (emphasis added) (footnote omitted).

196 California v. Greenwood, 486 U.S. 35, 40–41 (1988).

sight.[197] If the possessor of the effect has not excluded others by concealing the effect, then there is no expectation of privacy.

In the context of data trails, these traditional Fourth Amendment exceptions become rather distorted. Data trails are not really abandoned as much as in use when they leave the effect. Data packets are less digital trash at the curb, and more a digital package to be picked up and used by a third party. Nor is the data really in "plain view." Special devices are needed to intercept it, and data are rarely immediately incriminating, since the transmissions reveal nothing without translation and analysis. Thus, just as abandonment theory does not justify police opening a Federal Express package awaiting pick up or intercepting an encrypted email, it should not automatically apply to data trails (absent some exception or emergency).[198] Yet, the issue is far from resolved.

When it comes to digital analogues, it is not clear how the Supreme Court might address whether individuals have a reasonable expectation of privacy in data trails emanating from smart effects. Any of these doctrinal approaches could be applied, and like many Fourth Amendment questions the answer appears to be left to the Justices to choose as they see fit. This uncertainty in outcome has been a common complaint about the reasonable expectation of privacy test, and one that counsels for a new option.[199]

2. *"Houses" and Data Trails*

Principles of property and privacy combine to protect homes under the Fourth Amendment.[200] The Supreme Court

---

197 Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) ("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.").

198 That said, the Court has been willing to find no expectation of privacy for scents emanating from closed containers (through a dog sniff) and would presumably find other smells detected from a suspicious bag to fall outside the protection of a closed container. *See* Illinois v. Caballes, 543 U.S. 405, 409 (2005).

199 Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable."); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (complaining that the reasonable expectation of privacy test was really just "those expectations of privacy that this Court considers reasonable").

200 Payton v. New York, 445 U.S. 573, 589–90 (1980) ("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

has long emphasized the core understanding that "the Fourth Amendment stands [for] the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[201] The primacy of the home has been an oft repeated claim in Supreme Court cases[202]: "In no quarter does the Fourth Amendment apply with greater force than in our homes, our most private space which, for centuries, has been regarded as 'entitled to special protection.'"[203]

Even early on, however, the physical boundary of "houses" extended outwards to protect the homeowner beyond the four walls of the home. The principle of "curtilage" legally (and later constitutionally) created a buffer space immediately around the home that was treated like a home.[204] Curtilage has been defined to be the "area to which extends the intimate activity associated with the 'sanctity of a man's home.'"[205] As a historical matter, this expansion was required because many of the intimacies of early colonial life took place outside the physical home[206]:

> This dwelling area—called the curtilage—was readily discernible when the kitchen, the laundry, the springhouse, the woodshed, and most particularly the "outhouse" were not within the four walls of the mansion house. A man of the 19th Century . . . had the same right to resent being surprised by an intruder at 3 a.m. as he walked down the garden path to the privy as a man of the 20th Century . . . has a right to resent being surprised by an intruder at 3 a.m. as he walks

---

specific constitutional terms: 'The right of the people to be secure in their . . . houses . . . shall not be violated.'").

201 *Kyllo*, 533 U.S. at 31 (internal citations omitted); Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals.").

202 Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 913–14 (2010).

203 Kentucky v. King, 563 U.S. 452, 474 (2011) (quoting Georgia v. Randolph, 547 U.S. 103, 115 (2006)).

204 *See generally* Catherine Hancock, *Justice Powell's Garden: The* Ciraolo *Dissent and Fourth Amendment Protection for Curtilage-Home Privacy*, 44 SAN DIEGO L. REV. 551, 557 (2007) (detailing the Supreme Court's rejection of the personal and societal values embodied in curtilage and Justice Powell's dissenting view).

205 Oliver v. United States, 466 U.S. 170, 180 (1984) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

206 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.").

> down the hall to the bathroom. The expectation of privacy is constant; only the location of the "facility" has changed.[207]

Curtilage remains protected in the modern day, and the Supreme Court has elevated this ancient principle to constitutional status.[208] Curtilage currently receives similar protection as the actual home for Fourth Amendment purposes.[209]

Futuristic "smart homes" connected to the Internet of Things are becoming the showcase for sensor technology. Smart refrigerators, NEST Learning Thermometers, smart light bulbs, wall sockets, and heating systems have become the testing ground to imagine our integrated future.[210] In the smart home of the future, the lights will turn on as you enter the room, the heat will kick in when you enter the garage, your fridge will order milk when you run out, and your preferred ambient music will match your mood or activities.[211] Some of these innovations have the potential to save energy and money. Some are simply luxury. But, all will provide a rather revealing data trail of your daily habits, patterns, and preferences.[212] In addition, the data coming from tablets, laptop computers, printers, stereos, microwaves, and other Wi-Fi devices, including smart televisions and entertainment systems all can reveal equivalently personal details about the privacies of life inside

---

207 Charles E. Moylan, Jr., *The Fourth Amendment Inapplicable vs. the Fourth Amendment Satisfied: The Neglected Threshold of "So What?"*, 1 S. ILL. U. L.J. 75, 87 (1977).

208 United States v. Dunn, 480 U.S. 294, 301 (1987) ("[Curtilage] is so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection.").

209 Florida v. Jardines, 133 S. Ct. 1409, 1414–15 (2013) ("The officers were gathering information in an area belonging to Jardines and immediately surrounding his house—in the curtilage of the house, which we have held enjoys protection as part of the home itself."); *see, e.g.*, 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." (footnote omitted)).

210 Rutledge et al., *supra* note 28.

211 *Id.*

212 *See, e.g.*, 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 [https://perma.cc/U3JE-523C] ("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, 2002, 4:03 PM), http://www.nbcnews.com/id/45946984/ns/technology_and_science-security/t/smart-electricity-meters-can-be-used-spy-private-homes/ [https://perma.cc/NZ9T-HQTH] ("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.").

the home.[213] In short, the collected data trails from your home will reveal in intimate detail your daily patterns.

The answer to whether these data trails coming from one's home should be protected is relatively straightforward as a matter of Fourth Amendment precedent. In a series of cases applying both the physical intrusion/trespass test and the reasonable expectation of privacy test, the Supreme Court has protected most information emanating from a home. However, the reasoning of why this protection exists and how it would apply to data trails is less clear-cut.

a. *Data from Houses: Physical Intrusion/Trespass Test*

From a traditional physical intrusion perspective, any interception of data trails as a result of physically entering the house would be covered by the greater protection of the home. The threshold of the home remains a clear boundary to protect interception of data by law enforcement inside the home.[214]

This understanding was reaffirmed in *Florida v. Jardines*, although in the context of curtilage.[215] The question presented in *Jardines* was whether bringing a drug-sniffing dog onto the curtilage of a home to sniff for the scent of marijuana emanating from the home was a search for Fourth Amendment purposes.[216] Justice Scalia, doubling down on his physical intrusion theory in *Jones*,[217] stated, "The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections: When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'"[218] Because the dog crossed the threshold of the curtilage and gathered information, this amounted to a Fourth

---

213 Sometimes this information is literally intercepted by these smart devices. *See* David Goldman, *Your Samsung TV Is Eavesdropping on Your Private Conversations*, CNN MONEY (Feb. 10, 2015, 6:38 AM), http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/ [https://perma.cc/PX4X-WW8E].

214 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." (quoting Coolidge v. New Hampshire, 403 U.S. 443, 477 (1971))).

215 Florida v. Jardines, 133 S. Ct. 1409, 1410 (2013).

216 *Id.*

217 Technically Scalia changed his language from using the word "trespass" to the term "physical intrusion." *See* Kerr, *supra* note 119, at 91.

218 *Jardines*, 133 S. Ct. at 1414.

Amendment search.[219] This was so, even though the evidence (the scent of marijuana) had emanated from the inside of the house to the outside.

Jardines extended the traditional understanding that all searches of homes require a warrant to the curtilage.[220] Because the curtilage had been granted home-like protection, and because the dog was standing on the curtilage when it sniffed, this physical intrusion resolved the Fourth Amendment question.

In the context of data trails, this test would protect any interception of data from inside the curtilage (or within the home), but might not protect any interception from outside that protected space. If, for example, a police officer sniffed[221] out an unsecured Wi-Fi signal from the safety of her car, a strict reading of *Jardines* would offer no Fourth Amendment protection because there was no physical invasion or trespass of property. Under the application of a physical intrusion theory, some physical intrusion is still necessary to trigger Fourth Amendment protections.

b. *Data from Houses: Reasonable Expectation of Privacy Test*

Three concurring Justices in *Jardines* approved of Justice Scalia's property-based approach, but also signaled that the case could just have easily been decided on reasonable expectation of privacy grounds.[222] This outcome, they argued, had

---

219 *Id.* ("That principle renders this case a straightforward one. The officers were gathering information in an area belonging to Jardines and immediately surrounding his house—in the curtilage of the house, which we have held enjoys protection as part of the home itself. And they gathered that information by physically entering and occupying the area to engage in conduct not explicitly or implicitly permitted by the homeowner.").

220 *Id.* at 1414–15 ("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.' That principle has ancient and durable roots. Just as the distinction between the home and the open fields is 'as old as the common law,' so too is the identity of home and what Blackstone called the 'curtilage or homestall,' for the 'house protects and privileges all its branches and appurtenants.'" (internal citations omitted)).

221 *See generally* Shaina Hyder, *The Fourth Amendment and Government Interception of Unsecured Wireless Communications*, 28 BERKELEY TECH. L.J. 937, 939 (2013) (arguing that "the Fourth Amendment should prohibit the government from intercepting unsecured Wi-Fi signals"); Mani Potnuru, *Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 95 (2012) (noting that it is unclear whether unsecure Wi-Fi networks fall within the Federal Wiretap Act's protection).

222 Florida v. Jardines, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring) ("The Court today treats this case under a property rubric; I write separately to

been dictated ten years earlier when Justice Scalia himself wrote *Kyllo v. United States*, which expressly prohibited the technological interception of information from the home under a reasonable expectation of privacy test.[223]

Kyllo involved the use of a sense-enhancing thermal imaging device that could capture heat signals emanating from a home.[224] Police believed that Danny Kyllo was growing marijuana and that heat lamps could be detected using the thermal imaging device. An agent sat in his car and directed the thermal imaging device at Kyllo's home and recorded unusual heat patterns consistent with growing marijuana. The question was whether this use of technology to capture heat data was a search for Fourth Amendment purposes. In so holding, Justice Scalia reasoned,

> 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 protected area," . . . constitutes a search—at least where (as here) the technology in question is not in general public use.[225]

This was so even though the heat was captured leaving the house, was invisible to the naked eye, and didn't reveal many private details (except for the location of the heat sources). Going beyond the case at hand and foreseeing the danger of future technology that could invade constitutionally protected spaces and sources of private activity, Justice Scalia explained:

> But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house—and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves

---

note that I could just as happily have decided it by looking to Jardines' privacy interests.").

223 *Id.* at 1419 (Kagan, J., concurring) ("Jardines' home was his property; it was also his most intimate and familiar space. The analysis proceeding from each of those facts, as today's decision reveals, runs mostly along the same path. I can think of only one divergence: If we had decided this case on privacy grounds, we would have realized that *Kyllo v. United States*, 533 U.S. 27, 121 S. Ct. 2038, 150 L.Ed.2d 94 (2001), already resolved it.").

224 Kyllo v. United States, 533 U.S. 27, 29 (2001) ("In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex.").

225 *Id.* at 34 (internal citations omitted).

> that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.[226]

The concurring Justices in *Jardines* applied this reasoning to the marijuana scents emanating from the home into the curtilage to find that such information should also be protected under a reasonable expectation of privacy test.

Similarly, the data trails emanating from a smart house could be protected under a reasonable expectation of privacy theory. Just as the heat patterns in a house reveal personal information—as Justice Scalia memorably put it—including "at what hour each night the lady of the house takes her daily sauna and bath,"[227] the data patterns of when the bathroom light turns off, or the coffee pot turns on, or the fridge opens reveal personal information about the homeowner's daily patterns. Smart devices present exactly the type of technology that can "discern all human activity in the home."[228] This constitutional protection from exposure exists, even over the *Kyllo* dissenters' argument that "emissions from the outside of a dwelling" should not fall within the Fourth Amendment's language guaranteeing the people "to be secure *in* their . . . houses."[229] Information emanating from the house, even captured *outside* the house, falls within the protection of the Fourth Amendment.

Applying *Kyllo* to the Internet of Things, data trails from smart houses should remain protected under the traditional reasonable expectation of privacy approach. As with many things involving homes and the Fourth Amendment, the protection of a home remains strong even in a digital world.

3. *"Persons" and Data Trails*

The Fourth Amendment protects persons from being physically searched and seized.[230] Traditionally, this has meant

---

226 *Id.* at 35–36.

227 *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 in the house she went before and after that moment of relaxation.

228 *Id.* at 35–36.

229 *Id.* at 43 (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 (emphasis added)) is not only unprecedented but also quite difficult to take seriously.").

230 Terry v. Ohio, 392 U.S. 1, 19 n.16 (1968) ("Obviously, not all personal intercourse between policemen and citizens involves 'seizures' of persons. Only

that police need probable cause to arrest and to search a person's body, including inside his or her clothing,[231] and "reasonable suspicion" to physically seize his or her person.[232] In ordinary cases, this has meant that the human body and the information located on and around the human body has been designated a protected constitutional space. Physical intrusion into this space clearly implicates the Fourth Amendment. But, the protection has not been limited to invasions of the body or mere physical touching. Cases involving urinalysis collection have expanded the protections to the collection of biological material.[233] In the seizure context, the Supreme Court identified physical touching as the simple line to determine whether the Fourth Amendment has been implicated or not.[234] In the search context, the analysis has grown more complicated.

The early history of the Fourth Amendment offers little assistance in defining how the physical body—as a core protected space—should be protected. Obviously biometrics and genetic surveillance were not at issue, but even bodily invasions received little attention at the time of the Founding. As Professor Jules Epstein has noted,

> [T]he privacy concerns in 1792 and thereafter did not involve genetics or even invasions of one's body, but searches of a home or ship for papers or contraband or arrests (seizures) of a person. Searches of the person's clothing and possessions occurred appurtenant to lawful arrests and were accepted as an unquestioned right.[235]

Underlying this lack of concern for bodily searches was the reality that there was little evidence to be gained by searching the body in this early era. This assumption that the body cannot provide evidence in a criminal case has been refuted with the growth of fingerprinting, DNA testing, and other forensic

---

when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a 'seizure' has occurred.").

231 Minnesota v. Dickerson, 508 U.S. 366, 376 (1993).

232 *See Terry*, 392 U.S. at 19–20, 27 (creating test); *id.* at 37 (Douglas, J., dissenting) (describing majority's test as one based on "reasonable suspicion").

233 Maclin, *supra* note 209, at 140.

234 California v. Hodari D., 499 U.S. 621, 626 (1991) ("The word 'seizure' readily bears the meaning of a laying on of hands or application of physical force to restrain movement, even when it is ultimately unsuccessful.").

235 Jules Epstein, *"Genetic Surveillance"—The* Bogeyman *Response to Familial DNA Investigations*, 2009 U. ILL. J.L. TECH. & POL'Y 141, 149–50 (2009). Some scholars have even gone farther in arguing that protection of the personal body was not part of the original Fourth Amendment. *See* David E. Steinberg, *Sense-Enhanced Searches and the Irrelevance of the Fourth Amendment*, 16 WM. & MARY BILL RTS. J. 465, 480 (2007).

science.[236] Many cases now rise or fall on biological material removed from the human body.

Because health innovations have been at the forefront of the Internet of Things, questions about data trails from the human body raise fascinating constitutional issues. The "quantified self" movement—still, admittedly just developing—has focused largely on health innovation.[237] For example, implantable medical devices can monitor heart functioning, smart bandages can monitor the state of a healing wound, and fitness bands can measure the everyday patterns of sleeping, walking, and the wearer's corresponding heart rate.[238] Data trails emerging from inside your body (implantables), on your skin (smart bandages), and through a device attached to your wrist (a Fitbit or equivalent) provide a revealing profile about your current health.[239]

Are these data trails part of the person for Fourth Amendment purposes? Certainly the data coming from inside your body seems largely a manifestation of your person, but is it the same thing as your person for Fourth Amendment purposes? Is there a constitutional difference between a police officer placing his ear directly against your chest to listen to an elevated heartbeat, using a highly sensitive audio sensor to hear your heartbeat, or intercepting the digital trail of your Fitbit heartbeat? All of them reveal the same private information, but do they all constitute searches under the Fourth Amendment?

a. *Data from Persons: Physical Intrusion/Trespass Test*

Physically obtaining biological material from inside one's body has long been held to be a Fourth Amendment search.[240] In *Schmerber v. California*, the Supreme Court had to address whether the forcible withdrawal of blood constituted a Fourth

---

236 *See generally* Paul C. Giannelli, Ake v. Oklahoma*: The Right to Expert Assistance in a Post-*Daubert*, Post-DNA World*, 89 CORNELL L. REV. 1305, 1342–43 (2004) (noting that the growing importance of DNA evidence has led to legislatively and judicially created rights to expert assistance for defendants); Seth F. Kreimer & David Rudovsky, *Double Helix, Double Bind: Factual Innocence and Postconviction DNA Testing*, 151 U. PA. L. REV. 547, 553–54 (2002) (discussing the contested nature of access to DNA evidence in post-conviction proceedings).

237 *See supra* Part I.

238 Swan, *supra* note 32, at 218, 222 ("It is estimated that 80 million wearable sensors will be in use for health-related applications by 2017 . . . . These stretchable electronics track and wirelessly transmit information such as heart rate, brain activity, body temperature, and hydration level . . . .").

239 Olson, *supra* note 50.

240 Schmerber v. California, 384 U.S. 757, 767–72 (1966).

Amendment search.[241] In so holding, the Court reasoned, "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[242] While the search in *Schmerber* was held reasonable, the taking of blood to prove intoxication did constitute a Fourth Amendment search.[243]

In subsequent cases, compelled blood tests[244] and breathalyzers[245] have been understood to involve physical intrusions on persons for Fourth Amendment purposes. Any physical touching of the person to obtain evidence has been considered a Fourth Amendment search. "Persons" has also been extended to include clothing, items in pockets, undergarments, socks, and other extensions of the body. While these items could have been considered effects worn on the person, most courts simply referred to the protection of persons and looked to see if the items were physically examined. These early cases offer little help with the problem of data trails, as the interception of information from smart medical devices does not require physical intrusion into the body (or even pockets) of the suspects.

Of relevance to the analysis, however, is the Supreme Court's recent decision in *Grady v. North Carolina* applying the physical intrusion test from *Jones* to "persons."[246] In *Grady*, the Supreme Court held that the physical placement of a GPS monitor on a convicted sex offender under state-ordered monitoring is a search for Fourth Amendment purposes.[247] Citing *Jones* and *Jardines*, the Court held that "[i]n light of these decisions, it follows that a State also conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements."[248] Like *Jones*, central to the Court's reasoning was that the device

241 *Id.*

242 *Id.* at 767.

243 *Id.*

244 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616 (1989) ("We have long recognized that a 'compelled intrusio[n] into the body for blood to be analyzed for alcohol content' must be deemed a Fourth Amendment search.").

245 *Id.* at 616–17 ("Much the same is true of the breath-testing procedures . . . . 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 citations omitted)).

246 *See* Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015).

247 *Id.*

248 *Id.*

physically touched the individual, and also that the device was "designed to obtain information."[249]

Grady stands for the proposition that "persons" can be considered searched when, in fact, persons are not being physically searched (but are simply subject to the interception of personal data trails about their location). The key, however, at least from *Grady*, is that there is some physical intrusion/contact with the person to obtain the information. This reality obviously does not cover non-physical interception of data trails from smart devices located on persons.

b. *Data from Persons: Reasonable Expectation of Privacy Test*

With the exception of *Grady*, most of the Court's bodily integrity search cases occurred during the time when the reasonable expectation of privacy test was dominant.[250] In these earlier cases, the line between physical intrusion (drawing blood from the body) and non-physical intrusion (testing urine excreted from the body) remained blurred by this privacy focus. The Supreme Court was clear that physical intrusion into a body to obtain information violated a reasonable expectation of privacy, even if such a search is a relatively minor physical intrusion.[251] But the Court also protected bodily excretions such as breath or urine which have left the body and could be examined separately from the person. These cases—although arising out of the special needs doctrine—help guide the analysis of how the reasonable expectation of privacy test might protect data trails from smart devices in and on persons.

The Court's urinalysis decisions recognized that both the extraction of biological material and testing of that biological material involved an expectation of privacy.[252] By analogy, col-

---

249 *Id.* at 1371 ("The State's program is plainly designed to obtain information. And since it does so by physically intruding on a subject's body, it effects a Fourth Amendment search.").

250 *See Skinner*, 489 U.S. at 616 ("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. The ensuing chemical analysis of the sample to obtain physiological data is a further invasion of the tested employee's privacy interests." (internal citations omitted)).

251 *But see* Maryland v. King, 133 S. Ct. 1958, 1980 (2013) ("In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks.").

252 *See Skinner*, 489 U.S. at 617–18 ("Because it is clear that the collection and testing of urine intrudes upon expectations of privacy that society has long recognized as reasonable, the Federal Courts of Appeals have concluded unanimously,

lection of data trails from an embedded health device could be treated like bodily waste that, while no longer part of the person and not valuable in the traditional sense, still deserves privacy protection. If the content of one's vial of urine can claim a reasonable expectation of privacy, then so could the digital equivalent of personal health data.

Admittedly, tension exists in the doctrine surrounding biological material found outside the person. On the less protective side, collection of shed DNA has largely remained outside of Fourth Amendment protection, even though the revealing properties of genetic material are greater than those collected from breath or urine.[253] DNA, in fact, presents a difficult analogy for the puzzle of data trails. DNA on the person is obviously as protected as the person, just like data in a smart object is protected when it is within the smart effect. Courts, however, have initially been willing to separate out the protection of the person from shed DNA.[254] The shed DNA trail does not automatically gain the protection of the person once separated from the person. The data trail analogy would be that once separated from the smart device, the data loses the protection of the device. The result could be that biological trails and data trails could be collected without any Fourth Amendment check.[255]

---

and we agree, that these intrusions must be deemed searches under the Fourth Amendment.").

253 *See* David M. Jaros, *Preempting the Police*, 55 B.C. L. REV. 1149, 1180 (2014) ("Courts have uniformly rejected claims that the Fourth Amendment bars the police from collecting 'abandoned' or 'shed' DNA, and it is generally assumed that DNA profiles, once lawfully collected, can be retained and searched indefinitely." (footnote omitted)); *see also* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 866–69 (2006); Ken Strutin, *DNA and the Double Helix of Constitutional Rights*, N.Y. L.J., July 22, 2014, at 5.

254 *See, e.g.*, Williamson v. State, 993 A.2d 626, 634–35 (Md. 2010) (no expectation of privacy in DNA on discarded cup); Commonwealth v. Bly, 862 N.E.2d 341, 356–57 (Mass. 2007) (no expectation of privacy in DNA on cigarette butts and water bottle left in police interview room); State v. Athan, 158 P.3d 27, 37 (Wash. 2007) (no expectation of privacy in DNA on envelope mailed to detective); *see also* Joh, *supra* note 253, at 858 (discussing whether the Fourth Amendment protects individuals against government collection of samples of DNA that individuals leave behind).

255 Also on the less protective side, the sharing of biological and health data through smart devices provides an additional challenge to a reasonable expectation of privacy. One of the most common consumer devices in the Internet of Things has been a fitness monitor through a Fitbit, Apple Watch, or other device. This device attaches to a person's wrist and reveals biological health data to them and the contracting company. Consumers can voluntarily share the data with friends and family, although not usually with the government. The question of whether this data deserves a reasonable expectation of privacy is wide open due to the expanded audience of who has access to the data and the impact of the Third-Party Doctrine.

As a final piece of the puzzle, the concurring Justices in *Jones* supported the idea that aggregated, long-term collection of data trails can be a search for Fourth Amendment purposes.[256] If the long-term geolocational surveillance can be protected, one might imagine the long-term health information of a person would be even more closely protected. In fact, *Jones* provides an argument for expanding the reasonable expectation of privacy for persons beyond mere bodily integrity to a broader conception of personhood. In *Jones*, Justice Sotomayor eloquently explained the associational and expressive interests in being able to travel and live free from government surveillance, as well as referencing personal health information exposed by trips to clinics, surgeons, or psychiatrists.[257] These health choices and activities involve personal autonomy, family, religion, and other manners of self-expression.

Of course, the reality is that the Justices in *Jones* failed to resolve the hard questions of what that expectation of privacy would look like beyond the facts in *Jones*. While intercepting health data and long-term monitoring of health information from an individual's body intuitively seems invasive enough to violate an expectation of privacy, the current Court simply has not ruled on it.

4. *"Papers" and Data Trails*

The Fourth Amendment protects papers, reflecting the importance of freedom of thought, expression, and communication.[258] In an era of quill and paper and the primacy of the printed word, the Founders' documents, letters, books, and diaries could reveal deeply personal, overtly political, or associational sentiments.[259]

Historically, private papers, including documents and pamphlets that challenged governmental power served as a

---

256 *See* United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 962–63 (Alito, J., concurring).

257 *See id.* at 956 (Sotomayor, J., concurring) (citing People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

258 Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 122 (2007).

259 *See* United States v. Seljan, 547 F.3d 993, 1014 (9th Cir. 2008) (Kozinski, C.J., dissenting) ("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."); *see also id.* at 1018 ("The Founding generation recognized that the seizure of private papers also undermines freedom of speech.").

central point of contestation in the Founding era.[260] Famous English cases involving the search of papers seized to investigate and silence critics of the King received broad attention in the Colonies.[261] The case of John Wilkes, who was targeted for writing mocking articles about King George III, but who, in turn, sued the investigating officers for taking his papers, became a cause célèbre for the protection of private documents.[262] *Entick v. Carrington*, another British legal challenge protesting the seizure of private documents, has long served as the paradigmatic example of how confiscating private papers can chill free expression.[263] Entick, like Wilkes, challenged the search and seizure of his papers and won a symbolic victory for the right to dissent.

Protecting private papers, thus, became a central rallying cry in the creation of constitutional liberty.[264] Echoes of this concern can be observed in early state constitutions, and helped generate the Bill of Rights' explicit reference to unreasonable searches and seizures of papers (as distinct from effects).[265] Not surprisingly then, in the first cases involving the

---

260 *See* 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, 52 (2013) ("The Fourth Amendment refers to 'papers' because the Founders understood the seizure of papers to be an outrageous abuse distinct from general warrants.").

261 Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 875–76 (1985) ("The fourth amendment is based in large part on six celebrated English court decisions, including *Entick v. Carrington*, handed down in the two decades prior to the American Revolution. All six cases involved unsuccessful efforts by the English government to apprehend the authors and publishers of allegedly libelous publications, most notably the then famous *North Briton No. 45*. The decisions attracted considerable public attention in both England and the American colonies." (footnotes omitted)); Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. CIV. RTS.-CIV. LIBERTIES L. REV. 461, 463 (1981) ("Protection of private papers from governmental search and seizure is a principle that was recognized in England well before our Constitution was framed.").

262 *See* Schnapper, *supra* note 261, at 912–13 ("The Wilkes controversy also directly influenced the framers of the fourth amendment. The English search and seizure cases received extensive publicity in England and in America, and the Wilkes case was the subject of as much notoriety and comment in the colonies as it was in Britain. Wilkes' cause generated many supporters among American colonists, some of whom became key figures in the framing of the Constitution.").

263 *See* Dripps, *supra* note 260, at 72–75 ("We have long known that the tribulations of Wilkes were followed closely in the colonies . . . . The 'seizure of papers' was not an obscure issue of law; it was the stuff of everyday political conversation in the colonies.").

264 *See* TASLITZ, *supra* note 108, at 18 ("The abusive searches and seizures that captured colonial Americans' attention frequently involved state efforts to suppress dissent.").

265 *E.g.*, VA. DECLARATION OF RTS. § 10; MASS. DECLARATION OF RTS. § XIV; *see* Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue, 460 U.S. 575, 584

interpretation of the Fourth Amendment and private papers—*Ex parte Jackson*[266] and *Boyd*[267]—the Supreme Court had little difficulty in explaining the protection in clear and unequivocal terms. In *Ex parte Jackson*, the court reasoned that letters and sealed packages deserved protection: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[268] This protection continued even though the mailed letters had left the personal control of the sender. In *Boyd*, the court referenced *Entick* and the English cases declaring that a demand for documents under penalty of contempt was the equivalent of a search and seizure for Fourth Amendment purposes.[269] As discussed earlier, *Boyd*'s protection of commercial documents as "papers" exists as the high-water mark for constitutional protection, spurring a reconsideration and eventual rejection of such broad security of documentary evidence.[270]

Specifically, this protective vision of "papers" has been reconsidered through a series of cases which have expanded governmental power to compel the production of private papers through legal process, as well as to carve out exceptions to shared communications via the third party doctrine.[271] Documents can be subpoenaed.[272] Documentary privacy can be

---

(1983) ("The concerns voiced by the Antifederalists led to the adoption of the Bill of Rights."); Dripps, *supra* note 260, at 79 ("The want of a Bill of Rights was the central objection to the proposed Constitution of 1789, and this objection included explicit references to search and seizure.").

266 *Ex parte* Jackson, 96 U.S. 727 (1877).

267 Boyd v. United States, 116 U.S. 616 (1886).

268 *Ex parte* Jackson, 96 U.S. at 733.

269 Stuntz, *supra* note 109, at 423 (noting the Court's holding that the subpoena in *Boyd* was "the functional equivalent of a search or seizure"); *see* Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 592–93 (1996).

270 *See* Solove, *supra* note 258, at 138 ("The days of *Boyd* have long come to an end . . . . The third-party doctrine and doctrine on public surveillance have also severely curtailed the Fourth Amendment's protection of personal writings, reading habits, associations, and other First Amendment activities.").

271 For example, after *Miller v. United States*, 425 U.S. 435 (1976), Congress passed the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2013), and after *Smith v. Maryland*, 442 U.S. 735 (1979), Congress passed the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (2013).

272 *See* Hale v. Henkel, 201 U.S. 43, 73 (1906) (ruling that it was "quite clear that the search and seizure clause of the 4th Amendment was not intended to interfere with the power of courts to compel, through a *subpoena duces tecum*, the production, upon a trial in court, of documentary evidence").

deemed waived by revealing it to third parties.[273] Warrants for digital evidence can include essentially all of the digital files in a computer or device.[274] Business records, like those in *Boyd*, can no longer claim blanket protection under the Fourth or Fifth Amendments. While cases with countervailing constitutional claims involving freedom of the press,[275] political speech,[276] personal communication,[277] and liberty[278] have managed to preserve some protection, personal papers remain much less protected than under *Boyd*.

This constitutional reality presents a fascinating issue in an era of digital information. From one perspective, the Internet of Things can be reconceived as an ongoing paper trail of digital information. After all, a single smartphone can become the source of all letters (e-mail), documents (notes, diaries, work), books (e-readers), and dissenting pamphlets (angry hashtags or blog posts). In fact, one could conceive most smart objects in the Internet of Things as merely digital papers with coded information being created and shared.

Digital manifestations of documentary equivalents are everywhere. When individuals bank online, a digital paper trail equivalent to the old-fashioned deposit receipt is created. When individuals obtain prescription refills through their smartphone, a digital pharmaceutical receipt is created. When cars pass through an automated tollbooth, an electronic deposit and record of a transaction is created. Everything that

---

273 *See Miller*, 425 U.S. at 437–41 (1976) (finding no expectation of privacy in bank records shared with a third-party bank).

274 *See* Kerr, *supra* note 14, at 549.

275 *See* Stanford v. Texas, 379 U.S. 476, 485 (1965); *see also* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) ("Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" (quoting *Stanford*, 379 U.S. at 485)); Roaden v. Kentucky, 413 U.S. 496, 504 (1973) (holding that seizure of books and films is weighed differently under the Fourth Amendment than seizure of instruments of a crime).

276 *See* Lopez v. United States, 373 U.S. 427, 470 (1963) (Brennan, J., dissenting) ("[H]istorically the search and seizure power was used to suppress freedom of speech and of the press . . . . [F]reedom of speech is undermined where people fear to speak unconstrainedly in what they suppose to be the privacy of home and office." (internal citations omitted)).

277 *See id.* at 449 ("The right of privacy would mean little if it were limited to a person's solitary thoughts, and so fostered secretiveness. It must embrace a concept of the liberty of one's communications, and historically it has.").

278 *See* Sinclair v. United States, 279 U.S. 263, 292–93 (1929) ("Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value.").

the Founders had in their desks, we have in our computers. Further, all of the "paper" bank statements, prescriptions, library receipts, love letters, etc. have been replaced with digital counterparts.[279] If this documentary equivalent is taken seriously as digital papers, then the concept of Fourth Amendment papers may take a primary place in the protection of personal privacy or security.

In addition, formal communication has largely turned to digital means. E-mails, texts, and other social media communication have replaced letter writing.[280] The U.S. Postal Service handled about 150 billion pieces of mail in 2014, not an insignificant figure,[281] but only about the number of e-mails sent *every day* worldwide.[282] The same communicative purpose of letter writing has simply been transformed into digital form.

Finally, many personal reflections, creative thoughts, and political ideas are also written in digital form. The next political manifesto declaring independence will probably be drafted on a computer rather than on a scroll. The next public challenge to political corruption will likely be saved in digital storage rather than in a wooden desk. Yet, the substance of what is protected remains the same. The fact that paper was the form to capture ideas should not delimit the protection of Fourth Amendment "papers" to only that form. What matters was the protection of communication, expression, and dissent, not the ink and paper used to memorialize it.

Despite the growth of digital equivalents of papers, the Supreme Court is only just beginning to see how digital information may require a reworking of existing doctrine. The next two sections apply current Fourth Amendment law to this largely unresolved problem.

a. *Digital Papers: Physical Intrusion Theory*

Unlike *Jones*, *Jardines*, and *Grady*, the Supreme Court has not yet applied the physical intrusion test to a case involving

---

279 *See* Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 170–72 (2011).

280 *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (noting that email "is the technological scion of tangible mail"); United States v. Forrester, 512 F.3d 500, 511 (2008) ("The privacy interests in [mail and e-mail] are identical.").

281 *See* U.S. POSTAL SERVICE, POSTAL FACTS (2014), https://about.usps.com/who-we-are/postal-facts/postalfacts2014.pdf [https://perma.cc/K2Z7- R5ZE].

282 *See Inbox Overload: 182 Billion Emails Sent Daily Worldwide*, CBS NEWS (July 2, 2014, 1:52 AM), http://www.cbsnews.com/videos/inbox-overload-182-billion-emails-sent-daily-worldwide/ [https://perma.cc/2XUZJ9RT].

papers and new technology. Generally speaking, the interception of data in the form of papers (emails, texts, electronic receipts) would not involve any physical intrusion.

In *Riley*, the investigating officers physically manipulated the smartphone device, entering the passcode, scrolling through an address book, switching between photo applications, etc.[283] This type of physical touching likely is enough to constitute a physical invasion of digital papers. While *Riley* did not directly present that issue, the holding that such activity requires a warrant even incident to arrest likely means that the Court would consider such physical investigation a search for Fourth Amendment purposes absent an arrest.[284]

The physical intrusion test, however, would not provide protection if the same investigation could be done without physical contact. If police could access Riley's smartphone and retrieve information, either by tricking the device into sending data or hacking into it, a doctrinal gap remains about whether such a digital trespass constitutes a search.[285]

b. *Digital Papers: Reasonable Expectation of Privacy Test*

Riley broadly suggested that individuals have expectations of privacy in their digital papers without actually using the term "reasonable expectation of privacy." The language Chief Justice Roberts used evoked the privacy implications of this information without affirmatively relying on the traditional theory. In recognizing the qualitative and quantitative differences in smartphone data,[286] and the revealing nature of the information on the phone, the Court signaled a clear recognition that smart devices filled with the equivalent of digital papers would be granted some privacy protection. Equally important,

---

283 *See* Riley v. California, 134 S. Ct. 2473, 2480–81 (2014).

284 Arthur Leavens, *The Fourth Amendment and Surveillance in a Digital World*, 27 J. CIV. RTS. & ECON. DEV. 709, 719 n.52 (2015) ("In *Riley*, there was no question but that the data in the cell phone, the digital version of 'papers' or 'effects,' was protected by the Fourth Amendment; the question there was whether the cell-phone search that uncovered it required a warrant.").

285 Courts have not answered this question, and in a series of related cases involving malicious criminal hacking and other data breaches the issue of digital trespass has been debated with little consensus. Professor Orin Kerr, in a thoughtful essay, *The Norms of Computer Trespass*, sets out a framework for considering unauthorized computer access a criminal offense. *See* 116 COLUM. L. REV. 1143, 1153–61 (2016).

286 *Riley*, 134 S. Ct. at 2478 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person.").

the Court also recognized that the data trails existed separate from the smart effect itself (in the "cloud"), and yet despite being something else, deserved protection because of the connection to the effect.[287]

Similarly, in *Quon v. City of Ontario, California*, the Court assumed without deciding that individuals might have a reasonable expectation of privacy in the content of text messages (even messages sent on government issued pagers during work hours).[288] This was so regardless of the content (racy, sexually explicit messages) and despite the fact that the texts were held by third parties (the wireless company). The Court assumed without deciding that such messages, even in digital form, were the type of communication worth protecting.[289]

Both *Riley* and *Quon* could be read to adopt protection of the *content* of digital papers under a reasonable expectation of privacy theory, as opposed to the fact of the *communication* itself. Cases and commentary have long supported this distinction between content and communications data.[290] Telephone conversations and transmitting email have received Fourth Amendment protection.[291] Call logs and call lists have not received similar protection.[292] Similarly, the content of mailed letters remains protected even though the United States Post Office regularly scans the outside of all mail for postal addresses and keeps this information in a federal database without Fourth Amendment concern.[293] This distinction between content and non-content data also may be necessary in thinking about digital papers because of the role of the third party doctrine, which still controls the expectation of privacy for non-content information such as number dialed or other metadata.[294]

---

287 *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.").

288 130 S. Ct. 2619, 2630 (2010).

289 *Id.*

290 *See infra* section III.A.1.

291 *See supra* note 14.

292 *See supra* text accompanying notes 14–15.

293 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?_r=0 [https://perma.cc/XZ6EVUFW]; J.D. Tuccille, *Post Office Tracks Your Mail (Often Without Proper Authorization)*, REASON.COM (Oct. 28, 2014, 1:27 PM), http://reason.com/blog/2014/10/28/post-office-also-tracks-your-communicati [https://perma.cc/KL8D-QZUX].

294 *See* Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821, 824 (2014); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62

The question of whether interception of digital papers and communications violates a reasonable expectation of privacy remains unresolved. In some cases, courts have acted to protect digital information.[295] In others, they have not.[296] The addition of growing webs of metadata only increases the uncertainty. There may exist a different expectation in the privacy of one's email and the privacy of to whom the email was sent, but the courts have not agreed on how to draw the line for all digital papers and data signals.

Expectations may also depend on the content of the data. Digital medical records and bank records may be more reasonably protected than your daily receipts from Starbucks, which is why statutory protections covering medical and financial services have filled in the constitutional gaps.[297] But, such expectations remain complicated by the impact of the existing third party doctrine and strong law enforcement exceptions, which currently provide little reasonable expectation of privacy for records shared with third parties.[298] Finally, while *Riley* recognized the variety of digital information vulnerable to interception from our smartphones and the attendant privacy interests, *Riley* did not delineate any broader framework for how courts should treat this data.[299]

Simply stated, the Supreme Court has not definitively addressed digital papers in all their various forms. Virtual interception of data falls outside the physical intrusion paradigm,

---

STAN. L. REV. 1005, 1020 (2010); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2162–63 (2009).

295 *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (e-mail protected); *see also* Courtney M. Bowman, *A Way Forward After* Warshak*: Fourth Amendment Protections for E-mail*, 27 BERKELEY TECH. L.J. 809, 815–18 (2012) (discussing an earlier congressional attempt to protect digital privacy from the third-party doctrine).

296 United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (files in a file-sharing network not protected); United States v. Forrester, 512 F.3d 500, 509–11 (9th Cir. 2008) (Internet Protocol (IP) addresses and to/from e-mail information not protected).

297 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. *But see* Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1647 (2015) (highlighting that, through the advent of smartphones and other mobile devices, companies have been able to collect sensitive information from their customers, including their location, political preferences, communications with contacts, and other types of information).

298 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 (2013).

299 *See* Riley v. California, 134 S. Ct. 2473, 2489–91 (2014); *supra* notes 146–58 and accompanying text.

and the ubiquity of the information calls into question the reasonableness of any expectation of privacy. Echoes of concern can be heard in the concurrences in *Jones*[300] or the dicta in *Riley*[301] about how our digital lives reveal too much, but the Court has not yet settled on a way forward.

C. Reflections on the Current Doctrine: Sources and Security

Three important insights emerge from the foregoing analysis of the Fourth Amendment and data trails. First, the existing Fourth Amendment doctrine does not quite fit the digital age. A narrow reading of a physical intrusion/trespass test leaves many smart objects constitutionally unprotected. Further, privacy is an inapt organizing frame for data trails that regularly flow out of smart devices. By design, smart devices reveal private information to assist personal growth. The issue is not so much the privacy of data, but control of that data.

Second, unless the courts wish these ever-increasing data trails to exist outside constitutional control, a new Fourth Amendment theory for data trails must be created. While statutory and technological fixes remain possible, the choice to ignore constitutional implications may not be satisfying to courts or citizens.

Third, despite the doctrinal gap, the Supreme Court's two established search theories protect the same core interests which revolve around information and expression (self or associational) that emerges from persons, houses, papers, and effects. While stated in different terms, and with different language, the Supreme Court has repeatedly recognized the centrality of informational security coming from constitutionally protected sources.

The study of data trails and the Fourth Amendment highlights the importance of constitutional sources and informational security. The next section reexamines these two unifying themes as a foundation to build a more appropriate Fourth Amendment theory responsive to the challenges of sensorveillance.

---

300 *United States v.* Jones, 132 S. Ct. 945, 955–57 (2012) (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring); *see supra* notes 140–45 and accompanying text.

301 *Riley*, 134 S. Ct. at 2484–85; *supra* notes 146–58 and accompanying text.

III
A THEORY FOR PROTECTING SMART DATA UNDER THE FOURTH AMENDMENT

A "smart" Fourth Amendment must answer the question of whether data trails deserve constitutional protection. The current doctrine does not directly resolve the issue, but provides the building blocks for an argument to protect some (but not all) of these data trails.

This Part argues that protecting data trails from smart devices is consistent with the Fourth Amendment. Simply stated, at its core, the Fourth Amendment concerns itself with "informational security" arising from "constitutional sources." Defined here, "informational security" centers around personal information that is secured in some manner from governmental intrusion. Defined here, "constitutional sources" means the textually referenced, "persons, houses, papers, and effects."[302] Both concepts will be discussed in detail below, but broadly framed the idea emerges as a unifying principle to answer how data trails fit the Fourth Amendment.

As will be demonstrated, both the trespass/physical intrusion theory and the reasonable expectation of privacy theory seek to protect personal information deriving from constitutionally recognized sources. The former superficially focuses on the physical, property intrusion, the latter on the personal, privacy invasion. But, both at their deeper core protect something else besides property or privacy—they protect control over personal information.[303] This Part explains *why* data trails should be protected under the Fourth Amendment, and Part IV explains *how* the doctrine can adapt to this new digital age.

A. The Unifying Theme of Informational Security

The next few subsections develop "informational security" as a unifying theme among the otherwise divergent Fourth Amendment theories. As will be detailed, looking at the reason *why* the Supreme Court has protected certain constitutional

---

302 *See supra* note 3.

303 The reason for protecting Antoine Jones's car was not the minimal physical property interference, but the significant informational value of his travels. *See* United States v. Jones, 132 S. Ct. 945 (2012). The reason for protecting Charlie Katz's conversation in a public phone booth was not personal privacy (Katz was speaking in a quasi-public space to other listeners on the other end), but the informational value of the content of the call. *See* Katz v. United States, 389 U.S. 347 (1967).

interests leads directly to the conclusion that smart data falls within this protected class of information.

This discussion builds upon decades of scholarship by privacy law experts who have advocated for a focus on informational privacy.[304] Privacy law scholars have explicitly and implicitly, theoretically and practically articulated the foundational role of privacy behind Fourth Amendment doctrine.[305] As discussed later in subpart B, informational security provides a more limited, but more practical protection than infor-

304 DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 1 (2d ed. 2006) ("Information privacy concerns the collection, use, and disclosure of personal information. Information privacy is often contrasted with 'decisional privacy,' which concerns the freedom to make decisions about one's body and family. Decisional privacy involves matters such as contraception, procreation, abortion, and child rearing, and is at the center of a series of Supreme Court cases often referred to as substantive due process or the constitutional right to privacy."); *see also* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006) ("Information privacy draws primarily upon the tort law of privacy, state and federal privacy legislation, and constitutional protections guaranteed by the First and Fourth Amendments."); A. Michael Froomkin, *supra* note 22, at 1463 ("[W]hen possible, the law should facilitate informational privacy because the most effective way of controlling information about oneself is not to share it in the first place.").

305 *See, e.g.*, Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195 (2008) (proposing that a viable theory of privacy for the networked information age must consider the extent to which the "privacy of the home" has served as a sort of cultural shorthand for a broader privacy interest against exposure); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425–26 (2000) (explaining that the benefits of informational autonomy extend to a wide range of human activity and choice); Froomkin, *supra* note 22, at 1502 (theorizing that consumers suffer from privacy myopia, in which they sell their data too often and too cheaply); Richards, *supra* note 304, at 1089 (referencing the "Information Privacy Law Project," a collective effort by a group of scholars to identify a law of information privacy and to establish information privacy law as a valid field of scholarly inquiry); Schwartz, *supra* note 22, at 1612 (arguing that unfettered participation in democratic and other fora in cyberspace will not take place without the right kinds of legal limits on access to personal information); Paul M. Schwartz, *Privacy and Participation: Personal Information and the Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560–61 (1995) (arguing that data protection law must concern itself with decision making in deliberative autonomy and deliberative democracy); Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2177 & n.33 (2003) (emphasizing that various authors, independently of each other, have sought to develop information privacy laws based on the idea of privacy as a social good); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1093, 1125–29 (2002) (explaining that privacy should be conceptualized contextually as it is implicated in particular problems); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1204–05 (2002) (explaining how the Supreme Court has proclaimed that the constitutionally protected "zone of privacy" extends to decisional privacy and information privacy); Solove, *supra* note 22, at 1398 (explaining the "Big Brother" metaphor as the longstanding paradigm for conceptualizing privacy problems).

mational privacy and one that better addresses the problem of data trails.[306]

This section traces the theory of informational security through effects, houses, persons, and papers. The goal is to develop the argument that the Fourth Amendment should—consistent with traditional doctrine—protect personal information deriving from these constitutional sources.

1. *Effects and Informational Security*

Central to the protection granted effects has been securing personal information about those effects. The sparse Founding Era literature suggests a focus on protecting objects which revealed something about the owner—religion, culture, status, or family associations.[307] Searching and seizing a colonist's religious objects was not offensive simply because it interfered with property rights, but because searching revealed personal information about family and faith. Rummaging through bedroom drawers was not solely about the inviolate nature of property but, as the early history suggested, also about revealing information that might be contained in those drawers. Interpreted one way, the protection of effects has largely been the protection of what the personal effects revealed or contained.

Similarly, while Justice Scalia attempted to ground his *Jones* argument in property rights, the harm of affixing the GPS device was not in any real sense to physical property (the car was undamaged).[308] The real harm was exposing the revealing personal data about the effect (car). Placing the device on the car might have been a seizure, but what made it a *search* was collecting the locational data intercepted by police (the "use of that device to monitor the vehicle's movements").[309] The "use" in that case was the capturing of data trails via satellite transmissions communicated by cell phone to a government computer.[310] By using the car to track its owner, the government invaded the informational security of the effect. Justice Scalia's *Jones* analysis requires both parts—trespass

---

306 My focus on informational security addresses the centrality of informational control. The choice of prioritizing "security" over "privacy" has its origin in the work of Professor Tom Clancy and others who have argued that security provides a better frame of Fourth Amendment protection than privacy. *See infra* note 342.

307 *See supra* text accompanying notes 180–181.

308 *See* United States v. Jones, 132 S. Ct. 945, 948 (2012); *supra* subpart II.A.

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

310 *Id.* at 948 ("By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer.").

plus use—and as Justice Alito argues in his concurrence, neither alone should constitute a search under Scalia's reasoning.[311] In holding that this interception/collection was a Fourth Amendment search, Justice Scalia implicitly acknowledged the centrality of informational security.[312] What mattered was securing the information coming from the effect, not just securing the effect itself.

The concurring Justices in *Jones* also focused on the personal information revealed from the GPS device.[313] The reason a twenty-eight-day tracking of locational data became a search rested solely on the informational exposure that resulted. Such collection of personal data points (touching on associational, health, and other private travels) became of constitutional significance when the data trails could be revealing of private, personal actions.[314] The expectation of privacy was not about expectations from the effect (the car) itself, but the information to be inferred about the travels of the car. This personal information essentially radiating off the car is what created the constitutional harm.

Perhaps less protective, the traditional reasonable expectation of privacy test for effects—with its focus on closed containers and exceptions for publicly disclosed material—can be reconceptualized as only protecting the information secured ("concealed") from others.[315] Under the traditional doctrine, what is protected is the information inside the effect, less privacy of the effect itself. Individuals can only claim a reasonable expectation of privacy by taking steps to protect that information (placing it in a footlocker, parcel, or briefcase).[316] If the information is revealed to the outside world, then the plain view

---

311 *Id.* at 961 (Alito, J., concurring). While Justice Scalia does not address this argument, such a reading makes sense if we remember that the ultimate question is whether there was a search, not a seizure. Touching the car or putting the GPS device on the car might constitute a seizure of property (converting the property to government use), but for there to be a search, some information must be captured by government agents. In other words, if the police had stuck the GPS device on the car but no information could be collected, it would not be a search. If the police had simply collected the information without touching the car, it would not be a search.

312 *See supra* text accompanying notes 180–181.

313 Farahany, *supra* note 132, at 1249 ("The concurrences in *Jones* underscored that in the information age, defendants are less concerned about intrusions upon their real property and more concerned about intrusions upon their information.").

314 *See supra* subpart II.B.

315 *See supra* subpart II.A.

316 *See supra* subsection II.B.1.b. As may be evident, the logic of *Jones* and of the more traditional Fourth Amendment closed-container cases exists in some tension.

exception controls. If the information is voluntarily disclosed, then control over the information is deemed abandoned. In this way, the reasonable expectation of privacy of effects is really the reasonable expectation of information security about those effects. This reality would be so even in a world of x-rays and backscatter technology, which as a technical matter could expose the contents of a footlocker. The fact that a citizen is aware that such technology exists does not eviscerate an expectation of privacy in a closed container. What matters is not that the information, in fact, remains private, but the steps taken to secure (conceal) the information and exclude others from seeing it.

In studying effects, two points emerge: first, some effects are protected because of what information they reveal about the possessor of the effect, and second, some effects are only protected if steps are taken to maintain control of the information in the effect. But, both focus on the informational content and control of information from the physical object not just the physical protection of the object itself. Data from smart effects, thus, also should be protected as part of the informational security of the effect. As long as steps are taken to conceal, control, or secure the smart data, then it can claim some protection under the Fourth Amendment. As will be discussed in Part IV, such a claim presents practical difficulties, but as a conceptual matter, the data from smart effects can be protected as part of the effect itself.

2. *Houses and Informational Security*

A more obvious example of informational security can be seen in the Supreme Court's discussion of houses. The principle of protecting private property plainly influenced the Supreme Court's approach to homes.[317] But, the sanctity of what happens *inside* the home—information about the people and activities in the home—provides the true justification for why homes have been so privileged.[318] *Jardines* focused on

---

317 Boyd v. United States, 116 U.S. 616, 627 (1886) (recognizing that "[t]he great end for which men entered into society was to secure their property" (quoting Entick v. Carrington, 19 Howell's St. Tr. 1029 (1765))); Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

318 Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 MICH. L. REV. 889, 894 (2004) ("There has long been significant overlap between property rights

property control—who can exclude,[319] who had license to approach—as a mechanism to protect the activities inside the home.[320] *Kyllo* focused on expectations of privacy and the activities that could be revealed about what happens inside homes.[321] But both, at base, involved protecting the home as a space to allow human activities to flourish. And, neither involved merely the protection of the home as a physical structure independent of what happened inside the home. For that reason it is unsurprising that the protection of "the home" also covers spaces like apartments, hotels, and other places of personal privacy.[322] The surrounding form matters less than what happens inside.

Further, both lines of analysis protect information coming from the home that is no longer part of the home. Heat, conversations, and smells are protected because of their source (the home). The fact that they came from a constitutionally protected space is what controls. Emanations are not seen as separate from the source, but constitutionally protected because of the source. In the home context this is even true for not very private information (like heat use). As Justice Scalia said in *Kyllo*, "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[323]

Similarly, the protection of curtilage acknowledges that personal activities and private information can exist outside the home, and yet be covered by the Fourth Amendment protection of the home.[324] The derivative source of the home extends protections beyond the four walls to other personal

---

and reasonable expectations of privacy. Privacy is one of the things that people value about private property.").

319 David L. Callies & J. David Breemer, *The Right to Exclude Others from Private Property: A Fundamental Constitutional Right*, 3 WASH. U. J.L. & POL'Y 39, 58 (2000) ("The right of a landowner to exclude others is a fundamental part of the equally fundamental Constitutional Right to the enjoyment of private property.").

320 What was being protected in *Jardines* was private information (the scent of marijuana) coming from inside a person's home, but captured outside the home. *Jardines* shows that the Fourth Amendment recognizes a property-based protection of revealing information that comes from constitutional sources (homes), but have left (are emanating from) the source. *See supra* subsection II.B.2.a.

321 *See supra* text accompanying note 224.

322 Espinoza v. State, 454 S.E.2d 765, 767 (Ga. 1995) (apartments); Stoner v. California, 376 U.S. 483, 490 (1964) (hotels).

323 Kyllo v. United States, 533 U.S. 27, 37 (2001).

324 Ferguson, *supra* note 63, at 1287–88.

activities that happen nearby but clearly exist outside the home.

With homes, the principle of informational security becomes rather evident. Whether protecting information about activities inside the house, spaces near the house, or information about the house that can be captured radiating outside the four walls, the constitutional protection remains. Data trails emanating from the smart home, likewise, can claim a derivative protection of the home. Informational security principles apply both to the human activities and the digital manifestation of those activities originating from inside the home (even if collected outside the home).

3. *Persons and Informational Security*

Again, a unifying theme of protecting personal information emerges from the case law governing persons. *Katz*, the case that establishes that the Fourth Amendment protects "people, not places" was itself a case involving information being communicated by a person to another person.[325] The search at issue involved a conversation—words—captured at some remove from the person (the microphone was taped to the top of the phone booth).[326] Katz was neither touched nor even knew he had had his constitutional rights intruded upon. The protection ran toward the information leaving his person (via his mouth). The Fourth Amendment secured this information from interception.

Similarly, physically removing blood from a suspect is obviously a physical invasion of the person, but what is being regulated is not merely protection from getting jabbed with a needle, but protection of the revealing information in the blood (intoxication level, drug results). The Fourth Amendment protection is not just about bodily integrity but also security of biological information.

Likewise, the early reasonable expectation of privacy cases concerning drug testing of urine turn on the securing of personal, biological information.[327] Urine is generally considered abandoned. Once excreted, it is separate from the person. Yet, the reason we might still expect some security in its contents is because of the information it might reveal about the person

---

325 *See supra* section II.B.3.

326 Kerr, *supra* note 127, at 820 ("*Katz* began with an investigation into an illegal betting scheme. The FBI taped a microphone to the roof of a public phone booth used every morning by a suspect named Charles Katz.").

327 *See supra* section II.B.3.

(health status, pregnancy, drug use, etc.). The reason for protecting biological material from government collection (blood, urine, DNA) is primarily because of the potentially revealing information in the sample. For that reason, it may be the case that the shed DNA cases are erroneously decided[328] or perhaps only applicable to samples recovered from suspects after arrest (with a corresponding reduced expectation of privacy).[329]

Most interestingly, *Grady*'s extension of the *Jones* and *Jardines* rationale to persons reveals the importance of protecting informational security more than principles of property, dignity, or even privacy. *Grady* framed the placement of a GPS device on a person as being the search of a person, even though there was no actual bodily search.[330] *Grady* presents a perfect example of how Fourth Amendment doctrine is really about informational security. First, *Grady* was decided completely removed from the property-based justification that undergirds Justice Scalia's opinions in *Jones*/*Jardines*. Whereas *Jones* brought back considerations of trespass to chattel, and *Jardines* explicitly referenced property considerations of license, trespass, curtilage, and consent to homes, *Grady* involves no property concepts.[331] There was no concern of converting private property to government use. There was no concern of surreptitious collection that somehow interfered with property rights to use, exclude, or share. Instead, the Supreme Court simply extended the logic of *Jones*/*Jardines* to persons. And, in doing so, the Court resolved a pure case of information security. The only thing at issue in *Grady* was the information about where Grady might go (geolocational data). In holding that this collection of data trails constituted a Fourth Amendment search, the Court made the primacy of property give way to the primacy of informational security.

---

328 *See* Tracey Maclin, *Government Analysis of Shed DNA Is a Search Under the Fourth Amendment*, 48 TEX. TECH L. REV. 287, 312 (2016); *see also* Joh, *supra* note 253, at 882 ("The collection of abandoned DNA by police threatens the privacy rights of everyone."); Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 526 (2013) ("[T]he police conduct a search for Fourth Amendment purposes when they enter a cell, its nucleus, and the DNA therein to get identity information.").

329 Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 658 (2014) ("*King* did not directly address the collection, analysis, and retention of DNA samples from persons who have not been arrested for or convicted of a qualifying offense, leaving open the question of how the Fourth Amendment applies to crime victim, elimination, and suspect samples that have been volunteered to the police.").

330 Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015).

331 *Id.* at 1370–71.

Second, while the placement of the GPS band clearly involved physical contact, the harm was not simply to dignity,[332] but information-focused. As a convicted sex-offender, Grady was subject to far graver dignity harms than the placement of a tracking band on his body.[333] Instead, the constitutional objection recognized by the Court was the open-ended private information being revealed through a never-ending data trail. The search (as opposed to seizure) involved this private informational harm. *Grady* did not hold that the placement of a device on his body alone was the search, but placement with the intent to monitor the personal information about his whereabouts.

Finally, *Grady* was not decided based on *Katz* considerations. The five concurring Justices from *Jones* could have used the opportunity to decide on the reasonable expectation of privacy of a GPS band worn by a convicted sex offender. Instead, in deciding the case by extending the logic of *Jones*/*Jardines*, the Court appeared to accept that the tracking and interception of one's geolocational information through data trails was a search of the person for Fourth Amendment purposes.

These cases support the argument that the Fourth Amendment protects the informational security of persons. In the digital context, the informational security principles are strongest when talking about personal health, family, associational, and geolocational information. Whether from a smart medical device or a consumer fitness tracker, the informational security principles suggest that the Fourth Amendment covers this personal data originating from the person.

4. *Papers and Informational Security*

The Fourth Amendment's protection of papers presents the most straightforward example of informational security. The unifying theme connecting the papers in John Wilkes's desk and David Riley's smartphone involves the informational value

---

332 *See, e.g.*, Samson v. California, 547 U.S. 843, 847–49 (2006) (holding that parolees enjoy a reduced reasonable expectation of privacy due to their status as parolees).

333 *See, e.g.*, Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 373 (2014) (arguing that noncustodial restraints "can impose a form of de facto imprisonment" on sex offenders); Catherine L. Carpenter & Amy E. Beverlin, *The Evolution of Unconstitutionality in Sex Offender Registration Laws*, 63 HASTINGS L.J. 1071, 1122 (2012) (arguing that sex offender statutes are excessively punitive); Eric S. Janus & Wayne A. Logan, *Substantive Due Process and the Involuntary Confinement of Sexually Violent Predators*, 35 CONN. L. REV. 319, 338–59 (2003) (discussing sex offenders and their substantive due process rights).

of the documents, and not the format of memorializing those ideas.[334] The type of parchment or device matters little. What matters are the ideas revealed or recorded on those real and digital papers.

In all of the analysis of papers throughout the Supreme Court history, two themes emerge which largely support a broad protection of informational security in papers (and digital papers). First, the concern has never merely been the physical taking of papers; instead the concern has always been the protection of the ideas embodied in those papers.[335] Second, the security of papers was to encourage free expression and prevent self-censorship.[336] This freedom of expression included religious and political dissent,[337] but was also a recognition of the importance of intellectual growth encouraged by the development of new ideas.[338] Restrictions of such ideas not only undermine democratic liberty, but could also cause psychological harm that could be personally damaging.[339] Whether the government physically scrolls through a smartphone, looks in a desk, or virtually scans a computer, the threat to informational freedom and personal autonomy is the same. In considering the informational security of papers, the Court has always been concerned with securing a space of protection free from government surveillance. As such, because digital papers and attendant data trails reveal content of communications and other private opinions, they should also

---

334 *See supra* section II.B.4 & subsection II.B.4.a.

335 Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1105 (2006) ("Rather than merely prevent government seizure of the physical papers themselves, the Founders sought to prevent the broader harms associated with seizing the potentially sensitive information contained therein.").

336 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998) ("Simply put, surveillance leads to self-censorship.").

337 Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 434 (2008) ("Government surveillance—even the mere possibility of interested watching by the state—chills and warps the exercise of this interest. This effect was understood by the drafters of the Fourth Amendment, who grasped the relationship between preventing government searches of papers and protecting religious and political dissent.").

338 *Id.* at 436 ("Intellectual records—such as lists of Web sites visited, books owned, or terms entered into a search engine—are in a very real sense a partial transcript of the operation of a human mind. They implicate the freedom of thought and the freedom of intellectual exploration.").

339 Bradley, *supra* note 261, at 483 ("A search for private papers may be no more *physically* intrusive than a search for a gun, but the *psychological* intrusion is far greater, because the searcher is invading not only the subject's house but his or her thoughts as well." (emphasis in original)).

benefit from constitutional protections created to defend information and ideas.

5. *Informational Security from Constitutional Sources*

A theme of respecting informational security can thus be observed in the Supreme Court's interpretation of effects, houses, persons, and papers. In the forgoing analysis, informational security is not an abstract concept, but arises from those particular constitutionally referenced sources. The Fourth Amendment secures someone, something, or somewhere. Information obtained from a constitutionally recognized source—effects, houses, persons, papers—gains derivative protection due to the source of the information. Focusing attention on a derivative constitutional source provides a useful and relatively easy guidepost to identify which types of information deserve constitutional protection.

Such derivative protection also covers information at some remove from the actual constitutionally protected interest. Charlie Katz's voice exited the closed glass door and was captured by the microphone taped on top of the phone booth. Antoine Jones's travel coordinates left the car and was captured by satellite technology. David Riley's smartphone communications data existed both on the phone and outside of it (in the cloud). Yet, the protections of the Constitution carried to these intangible, invisible, separate pieces of personal information. The constitutional protections of persons, houses, papers, and effects might, thus, be better characterized as protections of the information emanating from those constitutionally protected interests.

B. Informational Security Defended

Informational security provides the organizing theory for applying Fourth Amendment principles to the problem of smart data. The data trails from smart objects exist as pure information. When arising from constitutional sources such as effects, houses, persons, and papers, this data lays claim to the Fourth Amendment protections sketched out above. The data becomes protected as an extension of the thing/place/person/paper itself. The data trail, if it is secured, and if it is the type of information traditionally protected by the Constitution, gets to claim this derivative, but equal, protection.

Why focus on security and not privacy? The reliance on the term "security" claims a long lineage in Fourth Amendment tradition. The constitutional text speaks of "the right of the

people to be *secure*."[340] The Founding Fathers used the principle of security in many of their early writings.[341] Professor Tom Clancy and others have argued that security, not privacy, has always been the controlling principle behind Fourth Amendment law.[342] In the Founders' world of physical surveillance and physical searches, the ability to physically exclude others defined a sense of security.

Informational security reflects the recognition that physical security, while important, may be less important in a digital age. Building a curtilage wall will not protect you from invasive visual, audio, and other surveillance. Police no longer need to break down your door to rummage through your papers when technology allows them to do the same thing from the comfort of their computers.[343] Yet, the constitutional right to exclude should remain, and the question for this Article and the larger problem of data trails is how to secure some of this information from the growing reach of sensorveillance.

The choice to rely on informational security is more limited than the broader theoretical protection of informational privacy.[344] Clearly privacy informs conceptions of security, but privacy expands out with a far greater reach. Privacy scholars have ably framed a broad and deep conception of informational

---

340 U.S. CONST. amend. IV, § 1 (emphasis added); *see* 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*.").

341 *See* Ferguson, *supra* note 63, at 1327–30 (discussing the history of being "secure").

342 *See* Clancy, *supra* note 109, at 322–23 (developing the concept of security as opposed to privacy as the controlling protection of the Fourth Amendment); Thomas K. Clancy, *The Importance of James Otis*, 82 MISS. L.J. 487, 505 (2013) ("The ability to exclude is so essential to the exercise of the right to be secure that it is proper to say that it is equivalent to the right—the right to be secure *is* the right to exclude. Without the ability to exclude, a person has no security. With the ability to exclude, a person has all that the Fourth Amendment promises: no unjustified intrusions by the government. In other words, the Fourth Amendment gives the right to say, 'No,' to the government's attempts to search and seize.").

343 *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting) (warning how the Fourth Amendment can be violated without physical seizure of information).

344 Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 231 (2005) ("Informational privacy is rooted in the Fourth Amendment's protection from unreasonable searches and seizures, as well as the conception of privacy outlined by Samuel Warren and Louis Brandeis in their famous 1890 article in the *Harvard Law Review*, where they used the phrase 'right to privacy' to denote a constellation of different interests, most of which involved the right not to have personal information exposed to the general public." (internal citations omitted)).

privacy, with many different and important facets.[345] Criminal justice scholars have also provided alternative visions of a privacy/security paradigm.[346] My concept of informational security offers a more modest approach, involving more practical concerns of exclusion, control, and access. Both security and privacy are important, but this Article emphasizes the former over the latter.[347]

---

345 *See, e.g.*, Richards, *supra* note 304, at 1134 ("'Privacy' is a particularly troubling term to use in the database context. On the one hand, virtually all scholars agree that 'privacy' is a concept that has eluded definition despite innumerable efforts to the contrary. On the other hand, privacy has come to be associated with a wide variety of meanings in addition to control over personal data, including residential solitude, rights of self-definition, freedom from government surveillance, and fundamental rights to make autonomous decisions about one's body."); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1107 (2014) (critiquing the idea of treating privacy as merely data flows and privacy as equivalent to informational privacy); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 134–40 (2007) (discussing the right to confidentiality in the United States); Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1156 (2011) (arguing for a more comprehensive regime of data security due to technological advances).

346 *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 18 (2007) (Proposing a test that looks at "whether law enforcement's proposed surveillance method is hidden, intrusive, continuous, and indiscriminate . . . ."); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71–72 (2013) ("[W]e argue here that Fourth Amendment interests in quantitative privacy demand that we focus on *how* information is gathered. In our view, the threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents." (emphasis in original)); Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. FORUM 10, 12 (2005) ("[W]hen an owner loses control of a copy of her data, she loses the ability to dispose of or alter that data, which I contend causes a form of seizure. This is analogous to the property right to destroy, which is tied to the rights of dominion and control. The Fourth Amendment prohibition on unreasonable seizure should protect these rights and provide a constitutional right to delete."); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 546–48 (2005) (arguing that privacy is not an indivisible commodity).

347 Finally, the term "informational security" resonates with the related fields of data protection and data security. "Data protection" has been adopted as the European conception of how best to consider data privacy. In other contexts, the term "informational security" relates to data breaches and other forms of guarding data from private collection or criminal interception. A world of informational security professionals work to guard access to data, build firewalls, and limit information from going to unintended sources. Richards, *supra* note 304, at 1136 ("'Data protection' is a somewhat technical concept that participants in the Information Privacy Law Project in the United States have used on occasion to describe the problems associated with personal data.").

The next Part seeks to operationalize an approach to analyzing data trails through the prism of "informational curtilage." The task of identifying these unifying themes is not meant to simplify the complexity of the Fourth Amendment. Scholars have identified many other controlling principles—dignity, respect, power, trust, intellectual privacy, legality—all of which are a part of the Fourth Amendment.[348] But, when focused on the problem of data trails, the principle of informational security serves as a more helpful guide. Part IV seeks to articulate how to apply that principle to the puzzle of data trails.

IV
INFORMATIONAL CURTILAGE

This Part develops a theory of the Fourth Amendment appropriate for the digital age. Building off the insight that informational security from constitutional sources provides a useful and constitutionally legitimate means to protect smart data, this Part adopts "informational curtilage" as a conceptual framework to guide future Fourth Amendment analysis.

In two prior articles I developed the theory of "personal curtilage" to carve out protection from "all seeing" surveillance technology in the physical world[349] and "digital curtilage" to protect smart objects in a virtual world.[350] This Article suggests a global theory of "informational curtilage" to augment those tests,[351] but also to replace the physical intrusion/trespass test and the reasonable expectation of privacy test currently in use.

---

348 *See, e.g.*, Jeremy M. Miller, *Dignity as a New Framework, Replacing the Right to Privacy*, 30 T. JEFFERSON L. REV. 1, 2 (2007) (human dignity); Andrew E. Taslitz, *Respect and the Fourth Amendment*, 94 J. CRIM. L. & CRIMINOLOGY 15, 98 (2003) (respect); Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1775 (1994) (trust); Richards, *supra* note 337, at 444 (intellectual privacy); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) ("power not privacy").

349 Ferguson, *supra* note 63, at 1287–88.

350 Ferguson, *supra* note 20, at 809.

351 Upon reflection, I have come to the conclusion that my previous theory of digital curtilage, *see id.*, may be too narrow a conception to cover the range of data related issues arising from the Internet of Things. The effects-based approach that undergirds digital curtilage may, in application, be too dependent on property concepts, and not sufficiently attuned to the fact that data is better conceived as information rather than property. The reworking of digital curtilage into informational curtilage is a recognition that the focus should be more on the data rather than the effect.

"Curtilage," as traditionally conceived, exists as a protective area around the home that secures the area from outside interference or observation.[352] Property and activities in this area gain derivative protection from the primacy of the home. As discussed earlier, the justification for this legal fiction[353] was to develop a space for personal and familial development free from outside intrusion. Stripped down to its essentials, curtilage is basically a recognition that certain constitutional sources (i.e., homes) deserve protection if the occupant has taken steps to build security (i.e., the symbolic curtilage wall), in order to protect the private activities that happen in and around the home.[354] The Supreme Court's test for physical curtilage echoes those principles requiring an analysis of four factors:

> [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.[355]

Informational curtilage expands this concept from the home to all of the constitutionally protected interests (persons, papers, effects), and focuses on the informational content not the particular physical space. Parallel to traditional curtilage, informational curtilage looks at the proximity/derivative connection to the constitutional source, the steps taken to mark out or protect the information, and the nature of the uses of that information.

The theory of informational curtilage answers the threshold question of whether the warrantless interception of data trails is a search for Fourth Amendment purposes. Informational curtilage defines the threshold of a protected data trail—the interception (and/or use) of which is a search.

---

352 United States v. Romano, 388 F. Supp. 101, 104 n.4 (E.D. Pa. 1975) ("The word curtilage is derived from the Latin cohors (a place enclosed around a yard) and the old French cortilliage or courtillage which today has been corrupted into courtyard. Originally it referred to the land and outbuildings immediately adjacent to a castle that were in turn surrounded by a high stone wall. Today its meaning has been extended to include any land or building immediately adjacent to a dwelling. Usually it is enclosed some way by a fence or shrubs." (citations omitted)).

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

354 Ferguson, *supra* note 63, at 1314–22 (discussing the history of curtilage).

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

A. The Theory of Informational Curtilage

The theory of informational curtilage provides an operational framework for courts to identify what information (including which data trails) deserves Fourth Amendment protection. To gain protection under an informational curtilage theory, three requirements must be met: (1) there must be a connection to a constitutionally protected source; (2) there must be a claim of security manifested by marking or securing the information from others; and (3) there must be an examination of the nature of the uses of the information. These requirements follow the traditional curtilage analysis well-established in the case law.[356] This subpart addresses how to define and apply each of the three elements of the informational curtilage theory. Consistent with the project of this Article, the analysis will focus on the problem of data trails, although the scope of the theory is not so limited.

1. *Connection to a Constitutionally Protected Source*

As established, the constitutional protections of houses, persons, papers, and effects have found a place of primacy in Fourth Amendment doctrine. Information (data) from those sources also, therefore, deserves primary protection.

The theory of informational curtilage first asks whether the information (data trails) at issue come from a home, a person, papers, or personal effects. Just as curtilage derives protection from the protection of the home, informational curtilage derives its protection from traditional constitutional sources. As discussed in Part II, Fourth Amendment cases regularly follow this approach. In a non-digital case, courts easily embrace the claim that because the information sought came from a person (e.g., urine), home (e.g., heat), or papers (e.g., incriminating documents), the Fourth Amendment applies.

The first step of an informational curtilage analysis merely asks if the information derives from a constitutional source. In digital cases, if so linked to a constitutional source, the data trails from that source will benefit from a derivative protection. This would include content data, metadata,[357] and all of the digital exhaust that remains from digital communication. Courts would merely look to see if the data trail came from one

---

356 *See supra* discussion at Part II.

357 *See generally* JEFFREY POMERANTZ, METADATA 3–13 (2015) (discussing the role of metadata in everyday life).

of these recognized constitutional sources. If not, the data falls outside of Fourth Amendment protection.

Analytically, this presents some differences in approach (if not outcome) with the current doctrine. Charlie Katz's phone call did not occur in his home or from his personal effects.[358] The only way that the informational curtilage theory would protect his communication would be to claim that the information derived from his person. Words coming from a person's mouth certainly qualify as information coming from a person. At least at this first level of analysis, direct interception of conversations would be protected because they derive from the textual protection of "persons"—a recognized constitutional source. Data trails from automobiles might be more protected under an informational curtilage theory than a *Katz* analysis because, while expectations of privacy in driving in public may be limited,[359] there is little doubt that cars are protected effects for Fourth Amendment purposes.[360] David Riley's smartphone data would be covered because it came from an effect. Similarly, Danny Kyllo's extra heat would be covered because it came from his home. But, some objects in the Internet of Things fall outside these textual sources and would not be covered.[361]

Generally speaking, however, this first element of analysis would provide a broad protection from direct interception. Most data trails sought by investigative agents would likely come from a person, home, effect, or papers. While issues of standing and control need to be examined (discussed next), the first analytical element tracks existing Fourth Amendment understandings applied to the digital world.

2. *A Claim of Security*

The second step of analysis asks whether the information has been secured in such a way to establish a barrier of control. Parallel to the curtilage wall erected to symbolically or

---

358 *See* Katz v. United States, 389 U.S. 347, 351–52 (1967).

359 *See* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"); *see also* United States v. Karo, 468 U.S. 705, 715–16 (1984) (describing whether property that has been withdrawn from public view is relevant to reasonable expectation of privacy).

360 *See supra* note 172 and accompanying text (discussing Jones' car as an effect).

361 Potentially most third-party sensors would fall outside of this protection. Direct interception of information from a smart device would be protected, but not the same interception from a third-party sensor.

literally mark out the curtilage, steps taken to protect the information from interception would be honored as a statement of security. What matters are the steps made to symbolize exclusion of others, rather than the reality of actually excluding others. After all, the fact that police can break in and defeat the security of a locked home does not undermine the constitutional protection of that home. The focus is again on informational control, rather than complete informational privacy.

The principle of informational security (discussed throughout this Article) can now do some real analytical work. As has been established, in the non-digital world, a defining aspect of what has been protected turned on what had been secured from others.[362] Justice Scalia's property preference rests implicitly on the property principle of exclusion.[363] Antoine Jones could control who could interfere with this car. Similarly, *Katz*'s statement that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected,"[364] the closed container doctrine, or the protection of the home, all turn on securing the information against another's access.[365] The key has always been whether one has attempted to exclude others from access to the information sought.[366] Hopping over a curtilage wall does not defeat the constitutional statement of security. One does not need a moat, only a symbolic wall marking out the area of security.

Security becomes even more important in the digital world. The theory of informational curtilage looks to see the steps taken to retain control over data or exclude others from data. A court would examine the practical, technological, legal, and other steps taken to ensure that data trails have been secured from others. The analysis would necessarily work along a continuum, with little to no protection for information freely shared with others (commenting through a public Twitter account), to more protection for users who controlled locational data access, restricted data sharing, and used encrypted ser-

---

362 *Cf.* Sklansky, *supra* note 345, at 1107 (describing privacy as "refuge," "[t]he notion that each of us needs 'a private enclave'—locations and aspects of our lives that are shielded from public scrutiny—may be a product of modernity, but it is so deeply entrenched that it has become part of what it means for a life to be well led and for a society to be well constituted" (internal citations omitted)).

363 *See supra* note 136 and accompanying text.

364 Katz v. United States, 389 U.S. 347, 351–52 (1967).

365 *See supra* note 195.

366 *Cf.* William C. Heffernan, *Property, Privacy, and the Fourth Amendment*, 60 BROOK. L. REV. 633, 643 (1994) ("What is critical to informational privacy, then, is not the presence of a physical 'shell' that contains facts about someone's life, but an individual's control over the dissemination of the facts themselves.").

vices, to absolute protection for people technologically savvy enough to use key encryption or establish contractual arrangements to secure data. Choices in data settings might signify security. Particular privacy policies might suggest limited access to others. Even temporary choices to turn off locational tracking or enhance privacy settings might be significant. The question will no longer be about expectations but about actions, and courts will need to examine the particular actions of the target.

Practically, this means that not all data trails will be granted Fourth Amendment protection. My smart umbrella which informs me about the weather might be secured if I have established settings to only share my locational data with the weather service, but not if any locational tracking device or service can find my umbrella. My smart car data might be secured if the contractual arrangement with my car company states that it will only use the data to alert me to repairs or in a service emergency, but not if I choose to share my car's location with everybody who offers me consumer assistance or services. Notice the issue is not whether I have given up privacy to one entity (and thus privacy to all entities), but how I have controlled access to my personal information. If the owner of the data takes steps to control the data and exclude others, then they can claim a measure of security over that data against others, including the government.

Of course, data trails are generated from sensors occasionally embedded (and sometimes hidden) in ordinary objects or devices.[367] Some devices will not be sophisticated enough to allow for controlling security features.[368] This technological limitation provides a significant constitutional limitation on data arising from the Internet of Things. Further, it might limit the protection of metadata or other digital signals unknowingly produced by the user. While metadata theoretically may gain protection because it derives from a constitutionally protected effect, as a practical matter it may not easily be secured. This is a big gap in coverage, and it is one that may not satisfy civil liberties advocates interested in more complete protection for metadata and related information. It also places a significant burden on those not technologically savvy enough to understand the security features on a smart device. Admittedly, unfair distinctions based on class and education may result in different levels of protection because of technological expertise.

---

367 *See* Shackelford et al., *supra* note 82, at 1, 14.

368 *Id.* at 14, 16.

In fact, all but the most technologically sophisticated user would likely reveal certain information as the unintentional byproduct of using particular technology.

This limitation, while real, may lead to a technological solution. As technology advances, many devices will allow users to control access to the information (even as default settings). If the concept of "informational curtilage" becomes adopted, companies may design products for such data security control.[369] In any event, users would not need to disable all such communications to retain security, but merely make an attempt to control access against intrusion. A curtilage wall has always allowed friendly guests to visit when asked, and such specific access does not also require general access for those not invited. Unlike expectations of privacy, which leads to the third-party doctrine exposure, security can be controlled, modulated, and enhanced by the individual.

Courts looking to see if the user has established a claim of security will look at the source of the data trail to see what the user has done to claim a measure of security. Did they allow open access to their data? Did they use encryption? Did they manifest through contractual arrangements or any other mechanisms, intent to keep this information secure?[370] The test will be objective because, of course, at the time of the judicial inquiry the person challenging the Fourth Amendment search will claim a subjective desire for security. But courts can look to see what steps had been taken to preserve this information from general consumption and interception.

This approach also has application in the physical world. In fact, the concept is so embedded in our lives that we do not notice it as a claim of informational security. We design houses with window shades and wear clothes that do not reveal our bodies. Those coverings exist to hide the information inside our homes and underneath our clothes. By securing the information from others, we demonstrate a claim to informational security. And, importantly, what is different about informational security compared to privacy is that even if the blinds are

---

369 Apple and Google have recently re-designed smartphones with new encryption software in response to weak legal protection of consumer data. *See* Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC (Sept. 19, 2014), http://www.bbc.com/news/technology-29276955 [https://perma.cc/8UR4-T9SH].

370 Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 614–16 (2015) (importing fiduciary norms and duties to protect third-party information).

slightly open,[371] or even if backscatter (x-ray-like) technology can see through our clothes, a claim to security protects us, even if we objectively have lost a measure of privacy. Individuals can control security through affirmative actions, and these actions do not depend on generalized understandings of privacy.

Such an information-based approach can be used to rethink seminal Fourth Amendment cases with sometimes different outcomes. By closing the glass door and paying his toll, Charlie Katz signified his expectation of informational security.[372] By securing his trash in an opaque bag on his curtilage, Billy Greenwood could make a strong claim of informational security because he took steps to secure his property from others.[373] By building fences and a mostly enclosed greenhouse on his property, Michael Riley could claim informational security from aerial surveillance.[374] These cases and others would now turn on the steps symbolizing security that the property owner took to protect the activities or information arising from these constitutionally recognized spaces. While only one factor in the informational curtilage test, this attempt to secure information as private would provide a stronger protection than the reasonable expectation of privacy test.

This reality opens up a related question about Fourth Amendment standing.[375] The current Fourth Amendment law relies on rather circular logic. If you have a reasonable expectation of privacy in the thing searched or seized, you can assert standing to suppress based on a violation of your reasonable expectation of privacy.[376] So a driver can assert standing in the search of her car, but a passenger with no ownership interest in that car cannot.[377] Because the informational curtilage theory exists separately from the reasonable expectation of privacy test, standing must be addressed.

---

371 Minnesota v. Carter, 525 U.S. 83, 87 (1998).

372 Katz v. United States, 389 U.S. 347, 351 (1967).

373 *See* California v. Greenwood, 486 U.S. 35, 39 (1988).

374 *See* Florida v. Riley, 488 U.S. 445, 463 (1989).

375 *See* Brendlin v. California, 551 U.S. 249, 259 (2007) (discussing a car passenger's standing under the Fourth Amendment despite the car belonging to someone else); Rakas v. Illinois, 439 U.S. 128, 138–39 (1978) (explaining that a defendant's Fourth Amendment rights are "invariably intertwined [with the] concept of standing"); *see also* Sarah L. Dickey, *The Anomaly of Passenger "Standing" to Suppress All Evidence Derived from Illegal Vehicle Seizures Under the Exclusionary Rule: Why the Conventional Wisdom of the Lower Courts Is Wrong*, 82 MISS. L.J. 183, 189 (2013) (providing background on the history of standing in Fourth Amendment jurisprudence).

376 *See Rakas*, 439 U.S. at 139.

377 *Id.*

Fortunately, the informational security principle addresses standing and ownership. Individuals who make a valid claim to informational security have standing irrespective of property ownership. Those who have the right to exclude others have the right to claim that right against the government for Fourth Amendment purposes. In fact, this principle is stronger than the current standing doctrine. If a claim of security were made, a lawful passenger could have the ability to exclude arresting officers from possessions in a car and thus have standing to contest the search.[378] After all, with the consent of the driver, a lawful passenger could exclude other uninvited guests ranging from hitchhikers to drunken friends from getting into a car. If a claim of security were made, short-term business associates in an apartment would be able to exclude others and thus claim security over the premises.[379] Even those individuals using private homes for commercial (and even illegal) operations could exclude neighbors and others from joining them.[380] Again, the issue would be what individuals did to claim a constitutionally recognized area as secure from others. A valid claim of informational security would equate to a valid claim of Fourth Amendment standing.

3. *Nature and Uses of Data*

The third factor in the informational curtilage framework turns on the nature of the uses of the data at issue. Not all information deserves Fourth Amendment protection, and the line drawn by the informational curtilage theory looks at the nature of the uses of the data.

The key is to look at why a particular constitutional interest is protected and why an attempt at security has been made. In a traditional curtilage analysis, the nature of the uses of the area became a factor because traditional curtilage existed to promote family and personal development around the home.[381] In constitutionalizing curtilage, the Supreme Court extended the surrounding areas that acted to protect these home-like/family uses. In the digital realm, the question becomes whether the data trail comes from a home or something that supports home-like activities. Data from a Nest Learning Ther-

---

378 The focus is on the search of the car, not the seizure. *Compare id.* (analyzing a third party's rights after an allegedly unlawful search of the owner's car) *with Brendlin*, 551 U.S. at 249 (analyzing a third party's rights after an unlawful stop of the owner's car).

379 *See* Minnesota v. Carter, 525 U.S. 83, 87 (1998).

380 *See id.*

381 *See supra* notes 353–54 and accompanying text.

mostat or equivalent would qualify because it reveals patterns of home life activities. Most of the smart home efficiencies (smart toasters, refrigerators, toothbrushes), in fact, would be protected because of the long-standing protection of data from homes. Courts would merely need to evaluate whether the nature of the uses of smart data from homes supports why we protect homes in the first place.

Importantly, the nature of constitutional interests is not the same. The protection of Fourth Amendment *papers* is less about family and home and more about personal, professional, or political expression.[382] A court examining whether digital papers should be protected under an informational curtilage theory would ask, not whether the data functions to protect the interests of curtilage (family/personal autonomy, etc.), but whether it protects the interests of papers (expression/creative freedom, business, dissent, etc.).[383] If so, then the nature and uses would be analogous and applicable. Under this analysis, encrypted email, notes, calendars, bank records, prescriptions, etc. would all be protected from direct interception, just like their non-digital counterparts. If the digital papers are the equivalent of ordinary Fourth Amendment "papers," they would fulfill the requirement of being the types of data that should be protected.

Similarly, a court examining whether to protect the data trails coming from persons—for example, a "smart" heart stent embedded in a patient—would ask whether the nature of the uses was the same as why the Fourth Amendment protects persons. Issues of human dignity, personal autonomy, and private health would suggest that such a protection should exist. Most smart medical devices would likely qualify for protection, as would most effects that revealed biological or health information.

Oddly, the hardest constitutional source to analyze might be effects. A court examining whether we should protect the data coming from a smart umbrella would need to ask why the

---

382 *See supra* discussion at section II.B.4.

383 This insight provides an important difference between the theories of "informational curtilage" and "digital curtilage." *See* Ferguson, *supra* note 20, at 866–68. Informational curtilage takes a broader view of the nature and uses of all of the constitutional sources in the text of the Fourth Amendment. The reason we protect persons is not the same as the reason we protect property. The theory of digital curtilage did not make that concession, adopting a more literal reading of the curtilage analogy. Informational curtilage takes its analogy not from the property concepts of curtilage but from the reasons why we protect persons, papers, and effects. It is thus a more expansive analysis of how curtilage principles should be applied to the digital world.

Fourth Amendment would protect a traditional effect. Both property and privacy considerations arise. In a prior article, I suggested that only effects associated with personal or private matters would deserve protection, relying on the Founders' preference to protect items found in homes.[384] This distinction presents some difficult line drawing that upon further reflection may be too limited. After all, Antoine Jones' car (effect) was considered protected. A broader understanding of protected effects may need to be created to address the expanding role of smart devices in our lives.

Yet, candidly the question of what types of smart effects should be protected has no easy answer. Courts will need to examine the type of effect at issue and determine whether the information from this type of effect deserves constitutional protection. A smart fork that reveals how fast you eat might get more protection than a smart tire that reveals the air pressure on your car. A smart fertility tracker might get more protection than a smart air filter that reports the toxins in the air. However, as detailed in Part II, the protection of unconcealed effects in public has never been robust, and thus protection of smart data from those effects may also be comparatively weak.

***

The theory of informational curtilage requires an analysis of all three elements, although in practice they regularly overlap. Any analysis of the nature and uses will raise an initial question of whether the data comes from a constitutionally protected space. Issues of what steps have been taken to secure the information might also inform the nature and uses question. And, of course, just because information comes from a constitutionally protected source and is consistent with the nature and uses of that source does not mean that the information will be protected; if no effort at security has been made, then there may be no protection.

Courts looking to answer the ultimate question of whether particular data trails are protected by the Fourth Amendment will need to ask: (1) if the data came from a constitutionally protected source (persons, houses, papers, or effects); (2) if the information was secured in some manner to symbolically or literally to exclude others; and (3) if the nature and uses of the

384 *See id.* at 870–72; Davies, *supra* note 107, at 714 (describing how originally the Fourth Amendment "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*" (emphasis added)).

data connects back to why we protect that particular constitutional interest in the first place. If the answer is yes to all questions, then the information is protected by the Fourth Amendment. If not, then the data falls outside of Fourth Amendment protection under an informational curtilage theory.

B. Capture and Collection

The final issue involves the capture of information. If the capture of data trails invades the threshold established by informational curtilage, it is a Fourth Amendment search. Informational curtilage provides a different threshold test, but the analysis tracks ordinary Fourth Amendment analysis. The question that remains, however, is whether law enforcement's capture of data must have been purposeful.

One of the complicated realities of sensorveillance is that the data streams exist all around us and can be intercepted inadvertently or for non-investigatory purposes. For example, during a natural disaster or fire, police might want to know the location of cellphone signals in an apartment building. Intercepting those signals would not be for investigatory purposes but emergency rescue.[385] If police officials needed to stagger traffic flow on a damaged bridge or during rush hour, intercepting data trails from cars might be considered a non-investigatory purpose.[386] More controversial examples might include intercepting information about prescriptions to warn of tainted medicine or intercepting energy usage to regulate electricity consumption during a severe heat wave.

This reality complicates the constitutional analysis, because the Supreme Court has been of two minds about the role of "purpose" behind Fourth Amendment searches. On one hand, the Supreme Court in *Grady* stated, "'the Fourth Amendment's protection extends beyond the sphere of criminal investigations,' and the government's *purpose* in collecting information does not control whether the method of collection constitutes a search."[387]

---

385 *See* Brigham City v. Stuart, 547 U.S. 398, 400 (2006) (discussing the public safety exception to the Fourth Amendment).

386 *See* Chandler v. Miller, 520 U.S. 305, 314 (1997) ("When . . . 'special needs'—concerns other than crime detection—are alleged in justification of a Fourth Amendment intrusion, courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties.").

387 Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015) (emphasis added) (citations omitted).

On the other hand, Fourth Amendment case law has often examined the purpose of police activity to determine whether it implicates constitutional rights.[388] In ordinary cases, the purpose is readily apparent as police officers are affirmatively investigating criminal activity. The vast majority of Fourth Amendment cases involve police officers targeting allegedly suspicious activities, suspicious people, or identified individuals or places of crime. Further, this purpose has been extended to non-criminal, civil cases involving civil regulation.[389] While not without internal conflict, civil investigations for regulatory compliance can trigger the Fourth Amendment when impacting constitutionally protected spaces. In these less traditional cases, the Supreme Court has looked to the investigatory purpose as a means of deciding the reasonableness of a search. Drug testing programs have been struck down when closely tied with criminal investigations[390] and permitted when focused on employment consequences.[391] Automobile checkpoints have been held to be unconstitutional when the "primary purpose" existed to investigate crimes[392] and permitted when the purpose was deemed regulatory in nature.[393] Outside the traditional "special needs" exceptions, the Supreme Court has excused police when acting as community caretakers,[394] emergency responders,[395] or in other regulatory

388 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) ("[W]e decline to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control.").

389 *See* Camara v. Mun. Court of San Francisco, 387 U.S. 523, 537–39 (1967) (explaining that the Fourth Amendment permits searches for certain civil administrative and public safety purposes).

390 *See* Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001).

391 *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 668 (1989).

392 *See Edmond*, 531 U.S. at 44.

393 *See* Illinois v. Lidster, 540 U.S. 419, 425 (2004) (upholding information-seeking traffic stops); *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451 (1990) (upholding police checkpoint stops for the purpose of preventing drunk driving).

394 Mincey v. Arizona, 437 U.S. 385, 392 (1978) ("Numerous state and federal cases have recognized that the Fourth Amendment does not bar police officers from making warrantless entries and searches when they reasonably believe that a person within is in need of immediate aid."); Cady v. Dombrowski, 413 U.S. 433, 441 (1973) ("Local police officers . . . frequently investigate vehicle accidents in which there is no claim of criminal liability and engage in what . . . may be described as community caretaking functions . . . .").

395 Brigham City v. Stuart, 547 U.S. 398, 400 (2006) ("[P]olice may enter a home without a warrant when they have an objectively reasonable basis for believing that an occupant is seriously injured or imminently threatened with such injury.").

roles.[396] The analytical dividing line has turned on examining whether or not the police action was done to investigate criminal/civil infractions or for some other governmental reason.

Further, as discussed in Part II, the Court in *Jones*, *Jardines*, and *Grady* emphasized that a search occurred when a constitutionally protected effect, home, or person was used to obtain information about that source. Explicit in the "use" analysis was that the police had the purpose to investigate. In *Jones*, the Court wrote, "It is important to be clear about what occurred in this case: The Government physically occupied private property for the *purpose* of obtaining information."[397] Scalia continued in a footnote to reiterate, "Trespass alone does not qualify, but there must be conjoined with that what was present here: *an attempt to find something or to obtain information*."[398] In *Jardines*, the Court wrote, "the question before the court is precisely [*whether*] the officer's conduct was an objectively reasonable search. As we have described, that depends upon whether the officers had an implied license to enter the porch, which in turn depends upon the *purpose* for which they entered."[399] In *Grady*, the Court cited the purpose language in *Jones* and stated, "In light of these decisions, it follows that a State also conducts a search when it attaches a device to a person's body, without consent, for the *purpose* of tracking that individual's movements."[400]

While the Supreme Court has stated that "governmental purpose" is not controlling, these lines of cases, involving traditional investigation and special needs investigation, share the commonality that they focus on the "purpose" of investigating wrongdoing. Because of that suggestion, the theory of informational curtilage follows this guidance. Under an informational curtilage theory, courts must ask whether the data was collected for the purpose of investigating criminal or civil wrongdoing. All direct surveillance would count. Most indirect surveillance that occurred during ongoing criminal investigations would count. Information collected under the pretext of a non-criminal investigation, but which is plainly a backdoor at-

396 *See* Chandler v. Miller, 520 U.S. 305, 314 (1997); *see also* Camara v. Mun. Court of San Francisco, 387 U.S. 523, 537–39 (1967).

397 United States v. Jones, 132 S. Ct. 945, 949 (2012) (emphasis added).

398 *Id.* at 951 n.5 (emphasis added).

399 Florida v. Jardines, 133 S. Ct. 1409, 1416–17 (2013) (emphasis added).

400 Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015) (emphasis added).

tempt at criminal investigation would count.[401] Some civil regulation by quasi-law enforcement agencies would count. However, certain non-investigatory collection might fall outside this law enforcement purpose.

CONCLUSION

This Article has offered a path forward to apply the Fourth Amendment to the problem of data trails. In a world that needs both smart devices and the Fourth Amendment, there also needs to be a new theory to protect the data trails we leave behind. Without such a theory, data trails will exist outside of Fourth Amendment protection, and an intrusive sensor surveillance system will be created without any constitutional restraints. Informational curtilage provides a workable test to distinguish the types of data that should be protected. As a test it emphasizes security over privacy and *ex ante* individual notice over *ex post* judicial review, and it provides a flexible balancing framework to allow for judicial discretion.

Equally important, theorizing data trails draws attention to the principle of informational security that underlies all of Fourth Amendment doctrine. While minimized in the case law and in tension with the property-focused direction of recent cases, informational security offers a superior analytical frame to understand why the Fourth Amendment protects certain things, areas, ideas, activities, and people. This article has sought to reclaim this insight and highlight it for courts and scholars. As new technologies develop in the Internet of Things and beyond, the hope is that these informational security principles can be applied to keep the Fourth Amendment smart enough to adapt to these challenges.

401 *See* Mills v. District of Columbia, 571 F.3d 1304, 1312 (D.C. Cir. 2009) (finding neighborhood checkpoints for automobile safety an attempt to avoid a constitutional prohibition of checkpoints for law enforcement purposes).