PACEMAKERS, FITBITS, AND THE FOURTH AMENDMENT: PRIVACY IMPLICATIONS FOR MEDICAL IMPLANTS AND WEARABLE TECHNOLOGY

Ashleigh Elizabeth Draft[*]

2019 MICH. ST. L. REV. 511

* Associate Editor, *Michigan State Law Review*; J.D. 2019, Michigan State University College of Law; M.A. 2008, Northern Illinois University; B.A. 2004, Calvin College. First and foremost, I would like to thank my husband Matthew and my children Greta and Sig for their unfailing support and encouragement during this project. I am also grateful to Professor Mark Totten, my expert reader, for his guidance throughout the writing and editing process. Finally, many thanks to my friends at the *Michigan State Law Review* who have improved this Comment in every way.

INTRODUCTION

Ross Compton of Middletown, Ohio, woke in the middle of the night as a fire spread through his house.[1] Although he knew he had to escape, he told the 911 dispatcher that he first collected some personal items, packed several suitcases, and threw them out his bedroom window before rushing out of the house.[2] However, Middletown police investigators doubted Compton's story, in part because the fire had started in several locations.[3] Compton was in poor health and relied on an artificial pacemaker to maintain his cardiac rhythms.[4] By collecting the electronic data from Compton's pacemaker—a noninvasive procedure that according to the deputy fire chief only required Compton to "give [them] his time"—investigators were able to see Compton's heart rate, pacemaker demand, and cardiac rhythms around the time of the fire.[5] The pacemaker data contradicted Compton's account of the fire, and the judge in Compton's criminal case subsequently allowed the data to be presented against Compton during his trial for insurance fraud and aggravated arson.[6]

Compton's case may have been among the first instances of a defendant's medical device data being used against him or her at trial.[7]

---

1. *See* Motion to Suppress at 2, State v. Compton, No. CR2016-12-1826 (Ohio Ct. C.P. Butler Cty. May 5, 2017).

2. *See* Karin Johnson, *Middletown Man's Electronic Heart Monitor Leads to His Arrest*, WLTW5 (Jan. 27, 2017, 8:08 PM), http://www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942 [https://perma.cc/UUZ7-V7X7].

3. *See id.*

4. *See id.*

5. Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told a Different Story*, WASH. POST (Feb. 8, 2017), https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.4ee2bd5484bd [https://perma.cc/P3FF-5M6U].

6. Order Denying Defendant's Motion to Suppress, Compton, No. CR2016-12-1826.

7. *See* Lauren Pack, *2 More Investigations Where Middletown Police Used Pacemaker Data*, J.-NEWS (July 14, 2017), http://www.journal-news.com/news/more-investigations-where-middletown-police-used-pacemaker-data/sfkuYvmupPkVj6vM2MBh0K/ [https://perma.cc/D2VF-PJYZ].

However, in the months since Compton's arrest, Middletown police have sought pacemaker data in at least two separate homicide investigations.[8] In the words of Middletown Police Lieutenant Jim Cunningham, "[e]verybody and everything out there now has a device with a lot of information in it."[9]

Medical devices such as cochlear implants and insulin pumps, along with wearable technology such as Fitbits and Apple watches, measure how people use their bodies.[10] In doing so, these devices track people's behavior and, by extension, record their choices throughout the day.[11] This data is valuable to consumers, medical professionals, and even law enforcement.[12] The Supreme Court, however, has not yet addressed the Fourth Amendment issues surrounding this personal health data.[13] This Comment analyzes the governing legal doctrines for personal health data that is stored locally on a consumer's device and data that is transmitted for monitoring to a third party.[14] Specifically, this Comment argues that society has heightened expectations of privacy for this data, and, accordingly, this data should be afforded greater Fourth Amendment protections.[15]

Part I discusses the health devices in question and how the data is collected and transmitted.[16] Part II summarizes the governing Fourth

8. *See id*.

9. *Id.*

10. *See* Simon Jary, *Fitbit vs Apple Watch*, TECH ADVISOR (Dec. 8, 2018), http://www.techadvisor.co.uk/feature/wearable-tech/fitbit-vs-apple-watch-2017-3612954/?p=2 [https://perma.cc/JSL2-NUPN] (describing how the Apple Watch and Fitbit track your level of physical activity, your heart rate, and your sleep); *see also* Mary Follette Story, *Medical Devices in Home Health Care*, *in* THE ROLE OF HUMAN FACTORS IN HOME HEALTH CARE 145 (2010) (ebook) (describing the increasing migration of medical monitoring into the home and listing types of home medical monitors); Ryan McCreery, *Data Logging and Hearing Aid Use*, 66 HEARING J. 18, 18–19 (2013).

11. *See* Jary, *supra* note 10.

12. *See* Story, *supra* note 10, at 148 (noting that some users of these devices are medical professionals, while others are lay caregivers or the care recipients themselves); Wootson, *supra* note 5 (providing an example of how this data is valuable to law enforcement).

13. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 552 (2017) ("The Supreme Court has only begun to explore the question of whether the Fourth Amendment needs a new digital understanding.").

14. *See infra* Sections III.A–B (analyzing the threshold question of Fourth Amendment protection for both locally stored data and transmitted data).

15. *See infra* Subsection III.B.2 (applying social norms for health and medical data to the privacy analysis for transmitted data).

16. *See infra* Sections I.A–B (detailing the types of medical and health trackers available, how they collect and store data, and why that data is valuable).

Amendment legal doctrines for these devices.[17] Part III examines legal issues that are unique to these devices and argues that when the data is stored locally on a device worn on or in the person's body, the Fourth Amendment should provide protections for this data that is coextensive with the protections provided to individuals' bodies.[18] Finally, it argues that the Court should carve out an exception to the third-party doctrine for data that is transmitted to a remote server for monitoring.[19]

I. MEDICAL AND HEALTH DATA: TRACKING AND PROTECTING

Continuous outpatient monitoring of patient data promises a revolution between patients and their physicians in the modern healthcare system.[20] Remote telemonitoring by medical professionals has various benefits:[21] it provides medical professionals with more reliable and consistent data versus patient self-reports;[22] it empowers patients through real-time feedback to adopt healthy behavior changes;[23] and it decreases healthcare costs by reliably monitoring patients away from the hospital.[24] At the same time, an increasing number of Americans are choosing to monitor their own health and wellness, as a majority of Americans now own some form of wearable technology like fitness trackers and smartwatches.[25] The number of

17. *See infra* Part II (describing the two predominant threshold tests in Fourth Amendment jurisprudence, the trespass test and the reasonable expectation of privacy test).

18. *See infra* Section III.A (analyzing the threshold question for locally stored data under both the trespass and privacy theories).

19. *See infra* Section III.B (analyzing the threshold question for transmitted data under both the trespass and privacy theories).

20. *See* Geoff Appelboom et al., *Smart Wearable Body Sensors for Patient Self-Assessment and Monitoring*, 72 ARCHIVES PUB. HEALTH, Aug. 22, 2014, at 1, 1.

21. *See id*. at 3–6.

22. *See id*. at 3 (describing patient self-reports as "unreliable and inconsistent for objective measurements" and providing an overview of clinical applications).

23. *See id*. at 6 (identifying the motivational aspects of health tracking and the way that patients "can become empowered to make healthy choices as preventative measures").

24. *Id*. at 3 ("If patients could be monitored reliably away from the hospital, this could decrease the cost associated with length of stay (LOS), which can greatly decrease healthcare costs and unintended consequences.").

25. Kari Paul, *Fitbit May Have Stumbled, but the Wearable Craze Isn't Dead Yet*, MARKETWATCH (Jan. 31, 2017), http://www.marketwatch.com/story/the-wearable-craze-isnt-dead-yet-2017-01-31 [https://perma.cc/JX6N-WTK6] ("[T]he majority of Americans now own wearables in some form, market research group Euromonitor found, including fitness trackers and smartwatches . . . .").

Americans who use wearable technology has increased dramatically in a short amount of time; in 2017, wearable fitness trackers and smartwatches could be found in 57% of American households, as compared to 26% of households just two years prior.[26] These medical and fitness devices collect data that is attractive to law enforcement, and certain the cultural expectations of privacy have become connected to this data.

A. Medical Devices and Their Consumer Counterparts

Medical devices that record and transmit patient data are proliferating.[27] Some of these devices aim to enhance doctor–patient communication and encourage people with chronic conditions to adopt healthy lifestyle changes.[28] The monitoring of insulin pumps for patients with diabetes, for instance, is one such use.[29] In contrast, some remotely monitored medical technologies, such as pacemakers, are necessary for the survival of the patient.[30] Pacemakers are implanted under the skin with electrical "leads" that enter the patient's heart.[31] These devices may use a home monitor that wirelessly receives the data stored on the implanted device; the home monitor then sends the patient's data to the physician via a landline, cellular, or wireless internet connection.[32] The patient may either manually direct his or her data to be uploaded using the device's software interface or the data may be continuously uploaded.[33] By examining the data from a

26. *Id.*

27. *See* Appelboom et al., *supra* note 20, at 3–4 (identifying clinical applications for cardiovascular monitoring, glucose monitoring, neurological monitoring, and physical therapy).

28. *See id*. (noting applications for patients with type one diabetes, Alzheimer's disease, and Parkinson's disease).

29. *See* Timothy S. Bailey, *Diabetes Data Management in the Clinic*, 1 J. DIABETES SCI. & TECH. 888, 889 (2007) (describing the practical application of remote glucose monitoring for patients in a diabetes clinic).

30. *See* Steve Stiles, *Remote Device Monitoring Cuts Mortality, Even for Pacemakers*, MEDSCAPE (May 9, 2014), https://www.medscape.com/viewarticle/824922 (noting that pacemaker patients with high remote monitoring use had a fifty-three percent greater survival rate than patients with low remote monitoring use).

31. *See Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter*, U.S. FOOD & DRUG ADMIN. (Jan. 9, 2017) [hereinafter FDA Safety Notice], https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm [https://perma.cc/ZU5G-8NXC].

32. *See id.*

33. *See id.*

patient's pacemaker, a physician is able to see time-stamped data indicating any periods of irregular heartbeats, as well as overall cardiac output.[34]

Cochlear implants and hearing aids are also medical devices that record patient data, logging how much time the user spends in different listening environments, such as quiet, noise, or speech in noise.[35] Moreover, some pharmaceutical companies are developing tracking devices that are physically ingested.[36] In November 2017, the Food and Drug Administration (FDA) approved the first "digital pill," a prescription medication embedded with a sensor that will inform doctors and family members whether patients have taken their medication as prescribed.[37]

Outside the medical context, American consumers have also demonstrated increasing interest in tracking their own health and fitness.[38] Around 2007, members of the "quantified-self" movement began to promote "self-knowledge through numbers" by using technology to track their personal data.[39] Members of the early quantified-self movement chose to track their steps, diet, sleep, and mood, among other metrics.[40] In 2008, Fitbit released its first activity tracker;[41] less than ten years later, 115.4 million wearable devices—

34. *See* Deanna Paul, *Your Pacemaker Can Now Testify Against You in Court*, WIRED (July 29, 2017), https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/ [https://perma.cc/A6EF-AFEC] (noting that data from a pacemaker can reveal heart rate and cardiac rhythms before, during and after a suspected crime).

35. *See* McCreery, *supra* note 10 (detailing clinical applications of this data monitoring and how it can affect the patient-provider relationship).

36. *See* Pam Belluck, *First Digital Pill Approved to Worries About Biomedical 'Big Brother'*, N.Y. TIMES (Nov. 13, 2017), https://www.nytimes.com/2017/11/13/health/digital-pill-fda.html?-r=0 [https://perma.cc/8SXV-GKQ7].

37. *See id*. The first application of this digital pill will be the antipsychotic drug Abilify. *See id*.

38. *See* Paul, *supra* note 25.

39. Gary Wolf, *What Is the Quantified Self?*, QUANTIFIED SELF (Mar. 3, 2011), http://quantifiedself.com/2011/03/what-is-the-quantified-self [https://perma.cc/AV4A-ZDLZ]; *see also* Gary Wolf, *The Quantified Self*, TED (June 2010), https://www.ted.com/talks/gary-wolf-the-quantified-self [https://perma.cc/5GVD-3FR8].

40. *See What Is the Quantified Self?*, *supra* note 39.

41. *See* Kate Greene, *Self Surveillance*, MIT TECH. REV. (Sept. 10, 2008), https://www.technologyreview.com/s/410806/self-surveillance/ [https://perma.cc/3AFK-RXF5].

including the Fitbit and Apple Watch—were sold worldwide in 2017.[42] Wearable devices may include a GPS sensor to monitor physical movement, an altimeter to monitor elevation gain, a heart rate sensor, or a skin temperature sensor.[43] For instance, the Ava Bracelet—designed to give the user greater control of her fertility—predicts the user's ovulation based on her body temperature and also tracks her sleep, physiological stress levels, and resting heart rate.[44]

These devices collect and store data in various ways.[45] Some devices, such as an insulin pump, store the user's data locally—on the device itself.[46] To be shared, an operator must manually share the data with an external database; ideally, this data is uploaded from the patient's home just before an office visit.[47] Other devices, such as pacemakers, may be remotely monitored as the data is continuously and automatically uploaded to a third-party database, like the Merlin.net Patient Care Network.[48] Consumer devices, such as a Fitbit or Apple Watch, store the data locally on the device and then sync to the user's phone, tablet, or computer.[49] Most Fitbit devices locally store minute-by-minute data for seven days and store daily totals for up to thirty days.[50] Fitbit devices may be set to sync this data every time the user opens the Fitbit application on his or her phone or periodically throughout the day.[51] However, whether health and medical data is stored locally or transmitted to a third-party server can

42. *See Forecast Wearables Unit Shipments Worldwide from 2014 to 2022*, STATISTA, https://www.statista.com/statistics/437871/wearables-worldwide-shipments/ [https://perma.cc/LMU8-2UWR] (last visited Mar. 11, 2019).

43. *See* Jary, *supra* note 10.

44. *See Ava Women*, AVA SCI. INC., http://www.avawomen.com [https://perma.cc/6K2L-BP8R] (last visited Mar. 11, 2019).

45. *See, e.g.*, Bailey, *supra* note 29, at 889; FDA Safety Notice, *supra* note 31 (describing how these devices collect and store data).

46. *See* Bailey, *supra* note 29, at 889.

47. *See id.*

48. *See* FDA Safety Notice, *supra* note 31. Pacemakers may also be equipped with continuous monitoring via Bluetooth wireless technology. *See A Bluetooth-Enabled Pacemaker Provides Flexibility to Patients*, CONE HEALTH MED. GRP. (Jan. 6, 2017), https://www.conehealthmedicalgroup.com/chmg/medical-services/heart-care/a-bluetooth-enabled-pacemaker-provides-flexibility-to-patients/ [https://perma.cc/VT69-2JRH].

49. *See How Do Fitbit Devices Sync Their Data?*, FITBIT [hereinafter FITBIT], https://help.fitbit.com/articles/en_US/Help_article/1877/?l=en_US&c=Topics%3ASyncing&fs=Search&pn=1 [https://perma.cc/RXA8-XSD8] (last visited Mar. 11, 2019).

50. *See id.*

51. *See id.*

have legal implications.[52] And, regardless of how the information is stored, consumers, physicians, and law enforcement have found this type of data to be increasingly useful.[53]

B. Value of Personal Health Data to Doctors, Consumers, and Law Enforcement

The objectivity of tracked medical and health data has made it attractive to medical professionals and law enforcement alike.[54] Traditionally, physicians have relied upon a patient's subjective self-reporting during an office visit to learn how the patient is doing at home or work.[55] However, these self-reported outcomes can be unreliable and may lack the consistency of objective measurements.[56] Continuous remote monitoring of a patient's physiological data has the benefit of accuracy, although only quantifiable data points can be monitored.[57] Physicians and patients also value the motivational aspect of health monitoring.[58] Under this model, patients become more informed participants in their health care and are more likely to take preventative steps to ensure their health.[59] Similarly, many casual

52. *See infra* Part III (employing the trespass theory and the reasonable expectation of privacy theory to analyze Fourth Amendment protections for locally stored and transmitted data). For an example of the locally stored versus transmitted data distinction in current government policy, see the June 2017 statement by Acting Commissioner for United States Customs and Border Patrol Kevin McAleenan specifying that border patrol agents may search data that is locally stored on a device but not data that is stored on an external server. *See Due Diligence Questions for Kevin McAleenan*, WASH. POST (June 20, 2017), https://www.washingtonpost.com/blogs/the-switch/files/2017/07/cbp-wyden.pdf [https://perma.cc/GEJ3-5S8J].

53. *See infra* Section I.B (explaining why consumers, medical professionals, and law enforcement value medical and health tracking data).

54. *See, e.g.*, Appelboom et al., *supra* note 20, at 2–6; *see also* Wootson, *supra* note 5 (providing examples of how this information is useful in both medical and law enforcement contexts).

55. *See* Appelboom et al., *supra* note 20, at 2–3.

56. *See id.* at 3.

57. *See id.* (describing a hybrid model in which the patient is "able to report their non-quantifiable variables while still having the ability to monitor quantifiable ones").

58. *See id*. at 1, 6 ("Studies show that a well-informed patient improves quality of life and patient outcome because they are more likely to participate in healthy behavioral changes.").

59. *See id.* at 6.

users of digital fitness trackers value a degree of accountability and motivation from their devices.[60]

Law enforcement may also value this data.[61] In the case of Ross Compton, the data from his pacemaker contradicted his own account of the fire that destroyed his home and belongings, and the judge allowed the pacemaker data to be entered into evidence against him.[62] Law enforcement also has used data from victims' devices to establish facts in a criminal investigation.[63] In Connecticut, police used a woman's Fitbit time-stamped data as a "silent witness" after her murder.[64] The woman's Fitbit tracker contradicted the account given by her husband, who was ultimately charged with her murder based partly on information from the woman's device.[65]

Law enforcement's access to this information will depend in part on the applicability of the Fourth Amendment.[66] When the victim or suspect consents to the search of his or her data during the course of a criminal investigation, Fourth Amendment privacy issues will not arise.[67] However, Fourth Amendment issues will arise when the victim or suspect chooses not to cooperate with law enforcement and does not consent to the search of his or her data.[68] In these instances, the

60. *See* Heidi Godman, *Can Digital Fitness Trackers Get You Moving?*, HARV. HEALTH BLOG (Aug. 27, 2015), https://www.health.harvard.edu/blog/can-digital-fitness-trackers-get-you-moving-201508278214 [https://perma.cc/G55M-2SNJ].

61. *See supra* notes 1–9 and accompanying text.

62. *See* Wootson, *supra* note 5; *see also* Brian A. Jackson, *Using Digital Data in Criminal Investigations: Where and How to Draw the Line?*, RAND BLOG (May 15, 2017), https://www.rand.org/blog/2017/05/using-digital-data-in-criminal-investigations-where.html [https://perma.cc/PQ3K-S5J5].

63. *See* Christine Hauser, *In Connecticut Murder Case, a Fitbit Is a Silent Witness*, N.Y. TIMES (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html [https://perma.cc/PR97-2WTK].

64. *Id.*

65. *See id.*

66. *See infra* Sections II.A–B for a discussion of the applicability of the Fourth Amendment.

67. *See* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 8.1 (5th ed. 2012). Consent may function "in lieu of obtaining a search warrant." *Id.* If valid consent is obtained, no probable cause or reasonable suspicion is required. *See id.* § 8.1 n.9.

68. *See id.* § 8.1; *see also* U.S. CONST. amend. IV. The Fourth Amendment protects "against unreasonable searches and seizures." *Id.*

amount of constitutional protection given will depend, in part, on social and cultural expectations of privacy for the data in question.[69]

C. Protecting Patient Privacy

For the last fifty years, American cultural expectations of privacy have been a prominent factor in courts' decisions about whether to extend Fourth Amendment protection in a given case.[70] The social norms surrounding personal medical and health information indicate that American society has heightened expectations of privacy for this data.[71] For instance, the Health Insurance Portability and Accountability Act (HIPAA) makes it an offense for a person to knowingly disclose individually identifiable health information to another person.[72] The legislative history surrounding HIPAA's passing in 1996 indicates that Congress was acutely aware of maintaining the privacy of individual medical and health information.[73] In the years following the HIPAA legislation, President Bill Clinton issued an executive order pertaining to law enforcement's use of protected health information,[74] in which he emphasized the importance of maintaining patient privacy as the government conducts health oversight and other business.[75]

The American Medical Association's (AMA) Code of Medical Ethics provides similar evidence of the social norms surrounding the privacy of medical and health information.[76] The code states that

69. *See infra* Section II.B (describing the Court's consideration of subjective and objective expectations of privacy).

70. *See infra* Section II.B (describing the shift in Fourth Amendment jurisprudence toward the "reasonable expectation of privacy" test).

71. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d (2012).

72. *See* § 1320d-6. An individual may not "use[] or cause[] to be used a unique health identifier; . . . obtain[] individually identifiable health information relating to an individual; or . . . disclose[] individually identifiable health information to another person." *Id.*

73. *See* Health Coverage Availability and Affordability Act of 1996, H. R. REP. NO. 104-496, at 100 (1996) (stating in a committee report that "[p]rotecting the privacy of individuals is paramount").

74. *See* To Protect the Privacy of Protected Health Information in Oversight Investigations, 65 Fed. Reg. 81,321, 81,321 (Dec. 26, 2000) (stating that the government "may not use protected health information concerning an individual that is discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations of a non-health oversight matter").

75. *See id.*

76. *See* AM. MED. ASS'N, CODE OF MEDICAL ETHICS §§ 3.1.1–3.1.5 (2016).

protecting patient privacy is a "core value in health care" and is "an expression of respect for patient autonomy and a prerequisite for trust."[77] Similarly, certain rules governing the admissibility of evidence protect communications between a physician and patient, and these rules have been vociferously defended in Congress, providing further evidence of heightened social norms.[78] Taken together, HIPAA, the AMA Code of Ethics, and the protections of patient–physician privilege illustrate that medical and health information are among the areas with the highest social norms for privacy protection.[79] Today, these devices and the data they collect must now interact with the Fourth Amendment, which was drafted more than two hundred years ago.[80]

II. GOVERNING LEGAL DOCTRINES FOR DEVICE DATA

The Fourth Amendment protects against unreasonable searches and seizures.[81] Through this Amendment, the government is limited in its ability to surveil its populace.[82] The American people expect and demand a degree of privacy from their government—a protection that facilitates self-expression, personal liberty, practices of religion and association, and other freedoms.[83]

A Fourth Amendment analysis of police or government conduct begins with two questions.[84] The threshold question is whether a

77. *Id.* § 3.1.1.

78. *See generally* Kenneth W. Graham, Jr. & Ann Murphy, *Rejected Rule 504: Patient's Privilege*, 25 FED. PRAC. & PROC. EVID. § 5521 (1st ed. 2018) (discussing proposed changes to rules of evidence that would affect patient–doctor confidentiality).

79. *See* Oliver v. United States, 466 U.S. 170, 178 (1984) (observing our "societal understanding that certain areas deserve the most scrupulous protection from government invasion").

80. *See Amendment IV: Search and Seizure*, NAT'L CONST. CTR., https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv [https://perma.cc/KU52-ZJME] (last visited Mar. 11, 2019). The Fourth Amendment was ratified in 1791. *See id.*

81. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

82. *See* Dale Carpenter, *Keeping Secrets*, 86 MINN. L. REV. 1097, 1098 (2002). The government "must answer democratically to a polity concerned about more than order." *Id.*

83. *See id.*; *see also* Ferguson, *supra* note 13, at 566.

84. *See* LAFAVE, *supra* note 67, § 2.1 (describing the first step of analysis as a determination of whether the government activity constitutes a search or seizure within the meaning of the Fourth Amendment).

search or seizure, as defined by Fourth Amendment jurisprudence, has occurred.[85] For the Fourth Amendment to apply, the government must conduct a search or a seizure.[86] If a search or seizure did occur, the second question is whether it complied with Fourth Amendment standards.[87] In other words, the second question asks whether the search was "reasonable."[88] In response to the second question, the Supreme Court in *Katz v. United States* ruled that the government's searches and seizures are per se unreasonable unless the search or seizure has been approved by the judiciary or falls within one of the exceptions established by the Supreme Court.[89]

A. The Threshold Question: Trespass Test

Contemporary Fourth Amendment jurisprudence contains two tests for answering the threshold question of whether a search or seizure has occurred: the trespass test and the reasonable expectation of privacy test.[90] Early jurisprudence framed the Fourth Amendment's protections as property protections against physical intrusion by the government.[91] In other words, for the Fourth Amendment to be triggered, the police must have intruded into a constitutionally protected area.[92] These protected areas were interpreted as those listed in the Fourth Amendment text itself: (1) "persons," including bodies and clothing; (2) "houses," including apartments and hotel rooms; (3) "papers," such as letters; and (4) "effects," such as automobiles or luggage.[93] In the 1928 decision *Olmstead v. United States*, the Court held that placing a wiretap on telephone wires outside of a suspect's home or office was not a search because the government did not

85. *Id*. ("Law enforcement practices are not required by the Fourth Amendment to be reasonable unless they are either 'searches' or 'seizures.'").

86. *See id*.; *see also* Ferguson, *supra* note 13, at 568.

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

88. *See id.*

89. *See* Katz v. United States, 389 U.S. 347, 357 (1967). Searches and seizures "conducted outside the judicial process, without prior approval by judge or magistrate" are "*per se* unreasonable under the Fourth Amendment—subject to only a few specifically established and well-delineated exceptions." *Id.*

90. This Section explores the trespass theory, primarily established by *Olmstead v. United States*, 277 U.S. 438, 465 (1928), and recently revived by *United States v. Jones*, 565 U.S. 400, 402 (2012). The *Katz* decision and the "reasonable expectation of privacy" test will be discussed *infra* Section II.B.

91. *See* LAFAVE, *supra* note 67, § 2.1(a).

92. *See* Silverman v. United States, 365 U.S. 505, 510 (1961).

93. *See* LAFAVE, *supra* note 67, § 2.1(a).

physically intrude into a constitutionally protected area.[94] This reasoning, that a search requires physical intrusion into a constitutionally protected area, was later superseded by the reasonable expectation of privacy test in *Katz*.[95]

Though for many years the trespass test was largely displaced by the privacy test established by *Katz*, the Court revived this physical intrusion test in *United States v. Jones*.[96] In *Jones,* police investigators placed a GPS tracking device on the underside of a vehicle registered to the defendant's wife while it was parked in a public lot.[97] Investigators then used the device to track the defendant's movements for twenty-eight days.[98] Based in part on the tracking information, the defendant was indicted on drug trafficking conspiracy charges.[99] The Court held that the placing of the GPS tracking device on the defendant's vehicle and its subsequent monitoring was a search for Fourth Amendment purposes.[100] The Court explained that while the *Katz* decision expanded the reach of the Fourth Amendment, the reasonable expectation of privacy test had not superseded the physical intrusion test.[101] Therefore, the Court held that when the government physically intrudes on a constitutionally protected area in order to obtain information, the Fourth Amendment regulates the intrusion.[102]

Jones concerned government intrusion into a specific constitutionally protected area—the defendant's automobile, or his "effects."[103] The Court's reasoning from *Jones* was used again in *Grady v. North Carolina* to support the finding of a government intrusion into a different constitutionally protected area—one's

94. *See Olmstead*, 277 U.S. at 465.

95. *See* LAFAVE, *supra* note 67, § 2.1(b).

96. *See id.* § 2.1(e). The *Katz* decision and the "reasonable expectation of privacy" test will be discussed *infra* Section II.B.

97. *See* United States v. Jones, 565 U.S. 400, 402 (2012).

98. *Id.* at 403.

99. *See id.*

100. *See id.* at 404.

101. *See id.* at 409 (noting that the reasonable expectation of privacy analysis has been "*added to*, not *substituted for*, the common-law trespassory test").

102. *See id.* at 407; *see also* Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475, 1503–04 ("[T]hough the majority in *Jones* concluded that the placement of a GPS device on a car violated the Fourth Amendment, this conclusion was based on a theory of trespass rather than on a reasonable expectation of privacy.").

103. *Jones*, 565 U.S. at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment.").

body.[104] In *Grady*, a convicted sex offender was ordered to participate in a satellite-monitoring program.[105] In this program, Grady would be forced to wear a tracking device at all times and be monitored for the rest of his life.[106] The state argued that the satellite-monitoring system did not entail a search within the meaning of the Fourth Amendment because participants in the sex offender program did not have a reasonable expectation of privacy regarding their whereabouts.[107] Relying on *Jones*, the Court disagreed and applied the trespass test to find that the satellite-monitoring system was a Fourth Amendment search.[108] The Court held that since the government's program was designed to obtain information, and it did so by physically intruding on Grady's body, it constituted a search within the meaning of the Fourth Amendment.[109]

Physical searches of the body in order to obtain biological material are also held to be Fourth Amendment searches.[110] For instance, compelled blood tests to determine intoxication trigger the Fourth Amendment both by the initial seizure of the person and the search that implicates the person's bodily integrity.[111] A search need not entail a "surgical intrusion" into the body, such as blood withdrawal, as the Court has held that the "deep lung" breaths required for a breathalyzer's chemical analysis are also searches.[112] Thus, under the physical intrusion theory as revived in *Jones*, physical searches of one's personal effects or one's body implicate the Fourth Amendment.[113]

---

104. *See* Grady v. North Carolina, 135 S. Ct. 1368, 1369–70 (2015). "[A] State . . . conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements." *Id.* at 1370.

105. *See id.* at 1369.

106. *See id.*

107. *See id.* at 1370.

108. *See id.* The Court also relied on the principle set forth in *Florida v. Jardines*, 569 U.S. 1, 5–6 (2013), which held that a search occurred when the police gathered information by physically entering and occupying the curtilage of a home without the homeowner's consent. *See Grady*, 135 S. Ct. at 1370.

109. *Grady*, 135 S. Ct. 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.").

110. *See* Ferguson, *supra* note 13, at 591.

111. *See* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 616 (1989).

112. *See id.*

113. *See, e.g.*, *Grady*, 135 S. Ct. at 1370 (applying the trespass theory to a GPS tracker worn on the body).

B. The Threshold Question: Reasonable Expectation of Privacy

The *Katz* decision in 1967 marked a significant shift in Fourth Amendment jurisprudence.[114] Katz was convicted of gambling and wagering offenses in violation of federal law, based in part on warrantless recordings of long-distance telephone calls he made from a public telephone booth.[115] Katz moved to suppress these police recordings.[116] The Court upheld his motion to suppress because although Katz did not have a property interest in the telephone booth, he was justified in expecting his conversations there would remain private.[117]

In *Katz*, the Court expanded Fourth Amendment protections beyond the established constitutionally protected areas, holding that "the Fourth Amendment protects people, not places."[118] The Harlan concurrence, which the Court subsequently adopted,[119] set forth a two-part rule.[120] In order for a search to trigger Fourth Amendment protections, a person must have exhibited a subjective expectation of privacy, and that expectation must be one that society recognizes as reasonable.[121] In contrast, the Fourth Amendment does not protect that which an individual "knowingly exposes" to the public.[122]

In *Kyllo v. United States*, the Court clarified that a Fourth Amendment search may occur without any physical intrusion at all.[123] *Kyllo* involved the use of thermal imaging to detect areas of heat emanating from a house because increased or unusual heat output may be evidence of an indoor marijuana-growing operation.[124] The *Kyllo* Court used the reasonable expectation of privacy test to hold that the

114. *See* LAFAVE, *supra* note 67, § 2.1(a) (describing the *Katz* decision as "landmark" and "seminal").

115. *See* Katz v. United States, 389 U.S. 347, 348 (1967).

116. *See id.*

117. *Id.* at 351–52 ("[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

118. *Id.* at 351.

119. Justice Harlan's test was adopted by the majority in *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).

120. *See* LAFAVE, *supra* note 67, § 2.1(b); *see also Katz*, 389 U.S. at 361 (Harlan, J., concurring).

121. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1171 (D. Or. 2012) (holding that a suspect had a reasonable expectation of privacy in the contents of his digital camera and an officer's warrantless search of the camera violated the Fourth Amendment).

122. *Katz*, 389 U.S. at 351.

123. *See* LAFAVE, *supra* note 67, § 2.2(e).

124. *See id.*

use of thermal imagers from a public street, pointed at a private house, constituted a search within the meaning of the Fourth Amendment.[125] Further, the Court held that using "sense-enhancing technology" to obtain information that could not otherwise have been obtained without physical intrusion into a constitutionally protected space is a search, as long as the sense-enhancing technology is "not in general public use."[126] As a result, *Kyllo* appears to endorse the proposition that the reasonable expectation of privacy—and, by extension, the protections of the Fourth Amendment—will shift as certain devices become more commonplace.[127]

Kyllo's caveat about technology "not in general public use" has been the subject of criticism.[128] Due to the onward march of technology, critics worry that as technology becomes more widely used and available, the protections the Court sought to extend in *Kyllo* will vanish.[129] In cases of DNA testing, contemporary technology and the privacy of the body intersect, and for many years, *Katz's* two-part rule—establishing protections for subjective exceptions of privacy that are objectively reasonable—has been employed to examine the expectations of privacy related to one's body.[130]

1. *Reasonable Expectation of Privacy: DNA Testing*

The Court has relied upon the reasonable expectation of privacy test to determine whether the collection of urine and DNA for chemical analysis constitutes a search within the meaning of the Fourth Amendment.[131] In *Skinner v. Railway Labor Executives'*

125. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001).

126. *Id.*

127. *See* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1394 (2002).

128. *Id.*

129. *Id.* at 1395 ("[T]he general use exception will eventually swallow the Court's newly minted prohibition of technologically enhanced investigation."). However, the Supreme Court recently denied certiorari in *State v. Worsham*, 227 So. 3d 602, 605–06 (Fla. Dist. Ct. App. 2017), letting stand a Florida appellate court decision that there is a reasonable expectation of privacy in the data contained in a vehicle's "event data recorder." *See* Florida v. Worsham, 138 S. Ct. 264 (2017) (denying certiorari).

130. LAFAVE, *supra* note 67, § 2.1(b) (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383 (1974)) ("Katz 'has rapidly become the basis of a new formula of Fourth Amendment coverage.'").

131. *See* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 617, 633 (1989) (holding that a mandated urine testing of employees was a search governed by the

Association, the Court held that mandated urine testing of railway personnel did constitute a search within the meaning of the Fourth Amendment because the collection and testing of urine implicated objective societal expectations of privacy.[132] Similarly, collection of DNA from an arrestee has been upheld as a search within the meaning of the Fourth Amendment, regardless of whether the DNA collection's purpose was to investigate a specific crime or to create a general police data bank for use in solving future crimes.[133]

However, the question of whether the Fourth Amendment governs the collection of DNA inadvertently shed by a person is more fraught.[134] It appears that shed DNA does not retain the protection of the person once it is separated from the person.[135] In *Williamson v. State*, the defendant was given a McDonald's meal while waiting to be booked at the police station.[136] After finishing his meal, the defendant discarded his cup and wrappers on the floor of the cell.[137] After he left the cell, officers entered and collected the cup, which they then submitted for a DNA test.[138] The DNA test yielded a match with evidence from prior sexual assaults.[139] Relying on the two-prong test from Justice Harlan's *Katz* concurrence, the court held that analyzing the DNA from the McDonald's cup was not a search because the

---

Fourth Amendment and the search was reasonable under the special needs doctrine); Yanez v. Romero, 619 F.2d 851, 854 (10th Cir. 1980) (holding that a urine test was a lawful search incident to arrest and threats by police officers to forcibly use a catheter if defendant did not voluntarily produce a urine sample did not deprive defendant of due process); State v. Thompson, 886 N.W.2d 224, 233 (Minn. 2016) (holding that a warrantless urine test does not fall within the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement).

132. *Skinner*, 489 U.S. at 617 ("[I]t is clear that the collection and testing of urine intrudes upon expectations of privacy that society has long recognized as reasonable.").

133. *See* LAFAVE, *supra* note 67, § 5.4(c); s*ee also* Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (holding that the warrantless swab of an arrestee's mouth for DNA evidence was a lawful search incident to arrest).

134. Mike Silvestri, Comment, *Naturally Shed DNA: The Fourth Amendment Implications in the Trail of Intimate Information We All Cannot Help but Leave Behind*, 41 U. BALT. L. REV. 165, 184 (2011) ("Naturally shed DNA, in the Fourth Amendment context, clearly presents a unique challenge for courts.").

135. *See* Ferguson, *supra* note 13, at 594.

136. *See* Williamson v. State, 993 A.2d 626, 630 (Md. 2010).

137. *See id.*

138. *See id.*

139. *See id.*

defendant had no reasonable expectation of privacy in what he had abandoned or voluntarily discarded.[140]

Unlike the defendant in *Williamson*, who was under arrest at the time of DNA collection, *Raynor v. State* addressed shed DNA collection from a suspect not under arrest.[141] Raynor voluntarily came to the police station for an interview after he was accused of sexual assault.[142] During his conversation with police, Raynor was asked to consent to a DNA test, to which he declined.[143] Raynor was wearing a t-shirt, and immediately after the interview an officer swabbed the arms of the chair where Raynor had been sitting and obtained a DNA sample.[144] Raynor conceded that the seizure of his DNA was lawful under the Fourth Amendment because he had no reasonable expectation of privacy concerning what he left behind on his chair.[145] However, Raynor argued that the search of his DNA by police required and lacked Fourth Amendment justification separate from the seizure of his DNA.[146] The court disagreed[147] and held that Raynor had no objective expectation of privacy in his DNA, in part because the police officers had only tested regions of the DNA strand that implicated Raynor's unique identity—not the areas of the DNA strand that carry "intimate genetic information."[148]

Similarly, in *United States v. Davis*, the Fourth Circuit Court of Appeals addressed the warrantless extraction of DNA from a suspect's clothing when the suspect was not under arrest.[149] The Fourth Circuit

---

140. *See id.* at 634; *see also* United States v. Cox, 428 F.2d 683, 687–88 (7th Cir. 1970) (holding that an inmate had no reasonable expectation of privacy in the hair that he voluntarily discarded after a haircut in prison); Commonwealth v. Bly, 862 N.E.2d 341, 356–57 (Mass. 2007) (holding that no search or seizure occurred when police analyzed the DNA on cigarette butts and a water bottle left behind in an interrogation room).

141. *See* Raynor v. State, 99 A.3d 753, 754 (Md. 2014), *cert. denied* 135 S. Ct. 1509 (2015).

142. *See id.*

143. *See id.*

144. *See id.*

145. *See id.* at 754–55.

146. *See id.*

147. *See id.* at 759. "[W]e hold that law enforcement's analysis of . . . petitioner's DNA left behind on the chair at the police station, in order to determine a match with the DNA the police collected from the scene of the rape, was not a search, as that term is employed in Fourth Amendment parlance." *Id.*

148. *See id.* at 761. "[T]he character of the information specifically sought and obtained from the DNA testing . . . is paramount in assessing the objective reasonableness of his asserted privacy interest." *Id.*

149. *See* United States v. Davis, 690 F.3d 226, 251 (4th Cir. 2012).

held that such extraction was a search in violation of the Fourth Amendment.[150] Years before he became a suspect himself, Davis was the victim of an unrelated shooting, and an officer collected his pants and boxers as evidence from Davis's hospital room—without a warrant or Davis's express permission.[151] The court held that the seizure of Davis's clothing was justified under the plain view exception, and Davis's expectation of privacy in his DNA was not implicated simply by cataloging the clothing as evidence.[152] Davis's clothing then sat in an evidence locker for four years.[153] Four years after Davis's shooting, a detective investigating a separate incident suspected Davis's involvement in a murder; the detective learned that a local police department had Davis's clothes and obtained the clothing without a warrant.[154] The detective was able to extract Davis's DNA from the bloodstain on his pants, and though the DNA sample was not useful for the detective's immediate purposes, it was entered into a local police DNA database where it was ultimately matched to a separate crime.[155] Davis challenged both the extraction of the DNA profile from his clothing and the subsequent retention of his DNA profile in the police database as violations of his Fourth Amendment rights.[156]

The Fourth Circuit held that the extraction of Davis's DNA profile from his clothing was an unreasonable search under the Fourth Amendment and assumed—without deciding—that there was a separate Fourth Amendment violation when his DNA profile was retained in the local database.[157] The court began its analysis with the threshold question of whether the removal of the DNA from Davis's pants constituted a search and concluded that it did.[158] The court reasoned that the extraction of DNA from Davis's pants was a search because Davis had a reasonable expectation of privacy in his DNA on the clothing.[159] In its holding, the court emphasized the type of analysis

150. *See id.* (holding that a Fourth Amendment violation occurred, but the exclusionary rule did not apply due to the good faith exception).

151. *See id.* at 230.

152. *See id.* at 239.

153. *See id.* at 231.

154. *See id.*

155. *See id.*

156. *See id.* at 232.

157. *See id.* at 232–33. *But see* State v. Athan, 158 P.3d 27, 31 (Wash. 2007) (affirming the conviction of a suspect who, prior to arrest, had been tricked into mailing a letter with his saliva on it to the police).

158. *See Davis*, 690 F.3d at 244.

159. *See id.*

that was conducted on the clothing and what potential information that analysis may reveal.[160] Unlike, for example, examining a piece of clothing for paint chips that match the paint from a crime scene, the analysis of biological samples can reveal private medical information.[161] The court also distinguished Davis's situation from those of individuals whose DNA is routinely collected after their arrest, incarceration, or parole, holding that a victim retains a greater privacy interest.[162] As a member of the public, Davis may reasonably have a greater expectation of privacy, unlike those whom the government has a greater interest in monitoring.[163]

Thus, due to the nature of the DNA analysis and Davis's status as a victim when his clothing came into police custody, the court concluded that Davis had a reasonable expectation of privacy in his DNA at the time it was extracted for analysis.[164] Since Davis had a reasonable expectation of privacy in his DNA, the extraction and analysis constituted a search under the meaning of the Fourth Amendment.[165] The court further held that the search of Davis's DNA was unreasonable in part due to its arbitrariness.[166] In contrast with the "programmatic nature" of the routine collection of DNA from arrestees or parolees, the search of Davis's DNA was conducted solely due to police suspicions that amounted to less than probable cause.[167] As a result, the search of Davis's DNA was a violation of the Fourth Amendment.[168] Expectations of privacy arise not only from social norms surrounding the privacy of one's body and genetic information but also from social norms surrounding the privacy of information that is shared, which is the heart of the third-party doctrine.[169]

---

160. *Id.* at 244 ("[W]e . . . must consider the type of analysis conducted on that clothing to determine whether Davis retained a reasonable expectation of privacy in his DNA on the clothing, or in the DNA profile obtained from it.").

161. *See id.*

162. *Id.* at 246 ("[A] victim retains a privacy interest in his or her DNA material, even if it is lawfully in police custody."). As of 2012, at least twenty-eight states enacted laws authorizing the collection of DNA from individuals following arrest or charging. David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095, 1095–96 (2013).

163. *See Davis*, 690 F.3d at 245 (discussing how the court held that Davis had a greater expectation of privacy than an individual whose "proven conduct substantially heightens the government's interest in monitoring them").

164. *See id.* at 246.

165. *See id.*

166. *See id.* at 249–50.

167. *Id.*

168. *See id.* at 250.

169. *See* LAFAVE, *supra* note 67, § 2.7(c).

2. *Reasonable Expectation of Privacy: The Third-Party Doctrine*

The third-party doctrine stems from the Court's assertion in *Katz* that the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public," even when that exposure occurs in one's own home or office.[170] In essence, the third-party doctrine states that people have no reasonable expectation of privacy in information that they voluntarily give to third parties.[171] As a result, law enforcement is able to utilize information that was released to a third party without probable cause or a warrant because the activity at issue is not a search and therefore is not governed by the Fourth Amendment.[172] For instance, the Court in *California v. Greenwood* held that individuals do not have a reasonable expectation of privacy in trash that they discard near the curb because the trash is knowingly exposed to a third party—in this case, the individuals' neighbors.[173]

The third-party doctrine's "secrecy model of privacy" has been criticized on both legal and practical grounds.[174] One legal argument is that the secrecy model of privacy improperly limits the protections of the Fourth Amendment by reducing privacy to an "all-or-nothing" proposition.[175] In this way, the third-party doctrine erases the distinction between information that is broadcast widely and information that is disclosed in a controlled environment, such as between a customer and his or her bank.[176] Justice Sotomayor's concurrence in *Jones v. United States* echoes this argument that secrecy should not be a "prerequisite for privacy," arguing that one should not assume the voluntary disclosure of information for a

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

171. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that a person does not have a reasonable expectation of privacy in phone numbers she dials in the privacy of her home). *But see* Klayman v. Obama, 142 F. Supp. 3d 172, 189–91 (D.D.C. 2015) (challenging metadata collection authorized by the U.S.A. PATRIOT Act).

172. *See* Richard M. Thompson II, CONG. RESEARCH SERV., *The Fourth Amendment Third-Party Doctrine* 1 (June 5, 2014); *see also* United States v. Miller, 425 U.S. 435, 437 (1976) (holding that bank consumers have no reasonable expectation of privacy in their bank records). *United States v. Dorsey* applies *Miller* to a defendant's recorded debit and credit card transactions. No. CR 14-328-CAS, 2015 WL 847395, at *18 (C.D. Cal. Feb. 23, 2015).

173. *See* California v. Greenwood, 486 U.S. 35, 40 (1988).

174. Thompson, *supra* note 172, at 2, 7.

175. *Id.* at 17; *see also Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

176. *See* Thompson, *supra* note 172, at 17.

limited purpose disqualifies that information from receiving Fourth Amendment protection.[177]

Justice Sotomayor's concurrence also references practical difficulties with the third-party doctrine in the digital age.[178] As she argues, in the course of daily life people reveal a significant amount of information about themselves to third parties.[179] The text of every Google search query is shared with a third party, namely Google itself, which also maintains a record of every email sent through their servers.[180] Third parties also hold data related to online sales transactions, social networking interactions, and shared photos with geotagged[181] locations.[182] These advancements in data generation and collection, paired with shifts in human interaction, mean that more information that previously would have been shielded by the Fourth Amendment is no longer protected.[183] The practical argument against the third-party doctrine also questions whether participation in these activities is truly voluntary.[184] In other words, use of a cell phone and online search queries may become so integrated into modern life that it would be unreasonable to require individuals to forego them simply to maintain Fourth Amendment protections over their information.[185]

Those arguing in support of the third-party doctrine liken the act of requesting evidence held by third parties to interviewing a witness after a crime.[186] In both instances, officers need not obtain a warrant to

177. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (arguing against the assumption that "all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection").

178. *See id.*

179. *See id.*

180. *See id.*

181. Geotagging is the process of adding location identification metadata to other types of media. *See* Olga Buchel & Diane Rasmussen Pennington, *Geospatial Analysis*, *in* THE SAGE HANDBOOK OF SOCIAL MEDIA RESEARCH METHODS 285, 292 (Luke Sloan & Anabel Quan-Haase eds., 2017). For instance, photos may contain embedded geographical information indicating where the photo was taken. *See id.*

182. *See* Thompson, *supra* note 172, at 2 n.12; *see also* David A. Harris, Riley v. California *and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 922 (2016). "The digital world, and the ways in which we can collect, store, analyze, and map the ever-growing pile of data produced on each of us every day is qualitatively different from what we can observe in the physical world." *Id.*

183. *See* Thompson, *supra* note 172, at 2.

184. *See id.* at 18.

185. *See id.* at 18–19.

186. *See id.* at 16.

receive assistance from a third party.[187] Further, Professor Orin Kerr[188] has argued that the third-party doctrine is an equalizer that allows law enforcement the same freedoms to investigate crime in the digital world that law enforcement officers enjoy in the natural world.[189] Kerr likens the metadata collected by third parties to the actions in the public square that would be in plain view of law enforcement.[190] Without technology, most crimes involve a public act in a space not constitutionally protected, such as purchasing drugs on the street, purchasing a weapon, committing sexual assault, or perpetrating other violent crimes.[191] In these cases, criminals must venture into a public space where the Fourth Amendment does not protect them.[192] Kerr worries that without the third-party doctrine, criminals may be able to conceal their activities from law enforcement by employing digital technology.[193]

Proponents of the third-party doctrine also argue that if the third-party doctrine is in error, Congress—not the courts—should extend protections to information shared with third parties.[194] Though Congress may not legislatively supersede the Court's interpretation and application of the Constitution, Congress may carve out its own role in constraining government surveillance.[195] For instance, a location-monitoring bill could prohibit companies from sharing a cell phone subscriber's location information unless the government

187. *See id.*

188. Professor Kerr is a Fourth Amendment scholar currently at the University of Southern California (USC) Gould School of Law. *See Orin Kerr*, USC GOULD SCH. L., https://gould.usc.edu/faculty/?id=73523 [https://perma.cc/H383-7W4H] (last visited Mar. 11, 2019). Prior to his appointment as a distinguished professor at USC, Professor Kerr was a professor of law at George Washington University Law School. *See id.* He has authored numerous books on criminal procedure and his scholarship has been cited by more than 3,000 academic articles. *See id.*

189. *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 575 (2009). "It corrects for the substitution effect of third parties that would otherwise allow savvy criminals to substitute a hidden third-party exchange for a previously public act." *Id.* at 561.

190. *See id.* at 575.

191. *See id.* at 574–75.

192. *Id.* at 575 ("[T]he wrongdoer has to leave his home and go out into spaces unprotected by the Fourth Amendment.").

193. *See id.*

194. *See* Thompson, *supra* note 172, at 26 (quoting Justice Alito that "a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way").

195. *See* Dickerson v. United States, 530 U.S. 428, 437 (2000) ("Congress may not legislatively supersede our decisions interpreting and applying the Constitution."); *see also* Thompson, *supra* note 172, at 25.

produces a warrant or acts under an exception to the warrant requirement.[196] In fact, Congress has taken a subject-matter-specific approach to limiting the third-party doctrine in the past.[197] The Electronic Communications Privacy Act of 1986—passed seven years after the Court's *Smith* decision applied the third-party doctrine to telephone records—contains provisions that require the government to seek a court order before using a "pen register" or similar device that monitors which telephone number a user has dialed.[198] Similarly, the Cable Communications Privacy Act of 1984 provides targeted privacy protection for cable subscribers, and the Stored Communications Act of 1986 establishes privacy requirements for "customer proprietary network information."[199]

In addition to these congressional acts, the Supreme Court has limited the scope of the third-party doctrine.[200] In *Ferguson v. City of Charleston*, the Court held that a hospital's sharing of drug test results with police without the patient's consent constituted an unreasonable search under the Fourth Amendment.[201] *Ferguson* concerned a public hospital program that entailed testing obstetric patients for cocaine use during pregnancy and after labor and turning over positive test results to law enforcement.[202] The hospital argued that the drug tests fit into a category of "special needs" searches because the aim of the program was to protect the health of fetuses and newborns.[203] The Court disagreed[204] and held that given law enforcement's close involvement with the program, the benign motive of protecting the health of mother and baby did not justify a departure from Fourth Amendment protections.[205] While hospital employees may provide police with

196. *See* Thompson, *supra* note 172, at 25.

197. *See id.*

198. *Id.* at 23. However, the language of the Electronic Communications Privacy Act removes discretion from the judge, directing the judge to issue the order "if the court finds that the attorney for the Government has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123 (2012).

199. *See* 47 U.S.C. § 222 (2012); 47 U.S.C. § 551 (2012).

200. *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001).

201. *See id.* at 85. The Court distinguished the hospital's mother–baby drug testing program from other "special needs" searches because "the hospital seeks to justify its authority to conduct drug tests and turn the results over to law enforcement agents without the knowledge or consent of the patients." *Id.* at 77–78.

202. *See id.* at 70–71.

203. *Id.* at 68.

204. *See id.* at 83. "[T]he immediate objective of the searches was to generate evidence for law enforcement purposes." *Id.*

205. *See id.* at 85.

evidence of criminal conduct they routinely acquire in the course of treatment, they may not turn over medical records to police without the patient's consent.[206] Even though one's medical records have been knowingly disclosed to a third party, the records are exempted from the third-party doctrine, and police may not access them without a warrant or patient consent.[207]

Importantly, the Supreme Court limited the scope of the third-party doctrine for digital data in *Carpenter v. United States*.[208] In *Carpenter*, law enforcement warrantlessly seized and searched historical cell site location information (CSLI) to reveal the whereabouts of Timothy Carpenter over the course of seven days.[209] The government obtained an average of 101 data points per day regarding Carpenter's location—painting a picture of his movements that the Court described as "encyclopedic."[210] The Court chose to analyze the government's actions under the *Katz* privacy theory, recognizing that digital data held by a third party does not fit neatly into existing precedents.[211] The Court declined to extend the third-party doctrine of *Smith* and *Miller* to the collection of deeply revealing digital data, holding that the government's collection of historical CSLI from Carpenter's cell phone provider was a Fourth Amendment search.[212]

In *Carpenter*, the Court distinguished CSLI from the bank and phone records at issue in *Smith* and *Miller*: historical CSLI is all-encompassing, creating numerous data points that are akin to wearing an ankle monitor; the "retrospective" quality of the information allows

206. *See id.* Justice Sotomayor referenced the *Ferguson* decision as an example of the third-party doctrine's limitation during oral arguments in *Carpenter v. United States*. *See* Transcript of Oral Argument at 23, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402).

207. *See* Transcript of Oral Argument, *supra* note 206, at 23; *see also* Edward J. Imwinkelried & D.H. Kaye, *Data Typing: Emerging or Neglected Issues*, 76 WASH. L. REV. 413, 435–36 (discussing the *Ferguson* case within the broader context of the third-party doctrine and distinguishing it from *Miller*).

208. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

209. *See id.* at 2217 n.3 (noting the total amount of data seized by the government covered many months, but the Court considered seven days to be the pertinent period). "It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.*

210. *See id.* at 2209, 2216.

211. *Id.* at 2214–15 ("[R]equests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.").

212. *Id.* at 11 ("We decline to extend *Smith* and *Miller* to cover these novel circumstances.").

law enforcement to search backward in time; the personal data can be accessed by law enforcement effortlessly, "with just the click of a button"; and data is not truly "shared" because the cell phone logs the information without any affirmative action on the part of the user.[213] Moreover, the Court emphasized the intimate nature of location information, noting that an individual's movements often reveal one's family, political, religious, and sexual associations.[214] However, the Court stressed that the *Carpenter* ruling is a narrow one that applies only to historical cell site location records and not, for instance, to real-time CSLI.[215] Looking ahead, the Court acknowledged many difficult questions related to personal data and emerging technologies, stating "we 'do not begin to claim all the answers today.'"[216] Thus, whether the third-party doctrine applies to personal health and medical data is a question the Supreme Court has yet to decide.[217]

III. PROVIDING HEIGHTENED FOURTH AMENDMENT PROTECTION FOR MEDICAL AND HEALTH TRACKING DEVICES

Constitutional protections for physical searches of the body were not among the Founders' foremost concerns.[218] Underlying this lack of concern was the fact that the government could gain little evidence from a suspect's body during this period.[219] However, with the growth of fingerprinting, DNA evidence, and forensic science, many criminal cases in recent decades have turned on evidence closely connected to the defendant's body.[220] Today, the recording of health and medical data has opened another door for evidence closely connected to the human body.[221]

213. *Id.* at 2217–18, 2220, 2223.

214. *Id.* at 2217 ("[T]hese location records 'hold for many Americans the privacies of life.'").

215. *Id.* at 17 ("Our decision today is a narrow one.").

216. *Id.* at 2217 n.4.

217. *See infra* Subsection III.B.2 for a discussion of whether the *Carpenter* reasoning would also apply to personal health and medical data that is transmitted to a third party.

218. *See* Ferguson, *supra* note 13, at 590.

219. *See id.* ("[T]he reality [was] that . . . little evidence [could] be gained by searching the body in this early era.").

220. *See id.* at 590–91.

221. *See supra* notes 20–44 and accompanying text (describing the nature and extent of data collected by health and medical trackers).

The recording of health and medical data presents unique legal issues for Fourth Amendment jurisprudence.[222] Whether the health and medical data is stored locally on a device or transmitted to a third-party server has legal implications for the search or seizure threshold question.[223] In each instance—whether the data is stored locally or transmitted—the application of the *Jones* trespass theory and the *Katz* privacy theory support enhancing Fourth Amendment protection for health and medical data.[224]

A. Is It a Search? The Threshold Question for Local Data

Data recorded by health and medical trackers is first stored locally on the device itself.[225] At that point, accessing the memory of the device is required to access the data.[226] Later, either through automatic transmission or patient-initiated transmission, the data is typically sent to third parties for storage on their server.[227] After transmission, anyone who has access to the third-party data bank may view the data, such as a medical professional who reviews the data before a patient appointment or a consumer who logs in to compare his or her health statistics from month to month.[228] This process of local storage followed by transmission creates two distinct moments

222. Ferguson, *supra* note 13, at 590–91 ("[Q]uestions about data trails from the human body raise fascinating constitutional issues.").

223. This is because the Court has held there is no reasonable expectation of privacy when data is "knowingly exposed" to a third party. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that a person does not have a reasonable expectation of privacy in phone numbers she dials in the privacy of her home). *See infra* Section III.A for an analysis of locally stored data and *see infra* Section III.B for an analysis of transmitted data.

224. *See generally* United States v. Jones 565 U.S. 400 (2012); Katz v. United States, 389 U.S. 347, 350–51 (1967). *See also infra* Subsection III.A.1 for an analysis of local data under the trespass theory and Subsection III.B.1 for an analysis of transmitted data under the trespass theory. *See infra* Subsection III.A.2 for an analysis of local data under the privacy theory and Subsection III.B.2 for an analysis of transmitted data under the privacy theory.

225. *See supra* notes 46–53 and accompanying text (describing how health and medical devices store and transmit data).

226. *See, e.g.*, FITBIT, *supra* note 49 (describing how certain consumer devices store data locally).

227. *See, e.g.*, FDA Safety Notice, *supra* note 31 (describing a cybersecurity vulnerability in a specific cardiac device and its accompanying transmitter).

228. *See supra* notes 47–53 and accompanying text (describing ways medical professionals and consumers can access the recorded data).

for Fourth Amendment analysis, depending on where the data is housed.[229]

1. *Local Storage: Threshold Analysis Under the Trespass Theory*

Under the *Jones* test, the government conducts a search within the meaning of the Fourth Amendment when it physically intrudes into a constitutionally protected area for the purpose of gathering information.[230] In *Jones*, the Court recognized a suspect's vehicle as a constitutionally protected area—an "effect" in the language of the Fourth Amendment drafters.[231] In *Grady*, the case concerning GPS monitoring of sex offenders, the Court recognized the body as a constitutionally protected area—a "person" in the language of the Fourth Amendment.[232] Medical and health devices combine elements of both "effects" and "persons."[233] Often, these devices are effects that are placed on people's bodies or even implanted inside their bodies.[234] Using the *Jones* and *Grady* precedents, the government's physical intrusion into a medical or health device located on or in one's body in order to gain information would likely constitute a search under the Fourth Amendment.[235]

However, physical intrusion, such as connecting a cable to the device, is not always needed to access the data stored locally.[236] For instance, in the *Compton* arson investigation, the investigators wirelessly collected data stored locally on Compton's pacemaker,

229. Data transmission, which is a form of information sharing, typically implicates the third-party doctrine. *See* Brief for the United States at 14–15, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402); *see also Carpenter*, 138 S. Ct. at 2206.

230. *See* United States v. Jones, 565 U.S. 400, 407 (2012).

231. *See id.* at 404.

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

233. *See supra* notes 30–44 and accompanying text (detailing how some devices, such as a pacemaker, are physically implanted into the body while others, such as a FitBit, are removable accessories).

234. Cochlear implants and pacemakers as examples of implanted devices, whereas Fitbits and Ava bracelets as examples of wearable devices. *See supra* notes 27–44 and accompanying text.

235. *See Grady*, 135 S. Ct. at 1370 (holding that forcing an individual to wear a GPS-monitoring ankle bracelet constituted a search within the meaning of the Fourth Amendment); *see also* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that a police officer may not warrantlessly search an arrestee's cell phone as part of a lawful search incident to arrest).

236. *See, e.g.*, *A Bluetooth-Enabled Pacemaker Provides Flexibility to Patients*, *supra* note 48 (explaining the Bluetooth-enabled pacemaker provided by Cone Health Medical Group).

requiring Compton only to sit in the room and "give [them] his time" while a machine downloaded the information.[237] Since *Jones* involved investigators physically touching the suspect's vehicle, and *Grady* involved court officials physically placing a GPS monitor on a sex offender, the Court has not yet ruled on an instance where the government initiates a *wireless* intrusion on an individual's body or effect.[238]

However, the Court's 2001 *Kyllo* decision *did* address a nonphysical intrusion into a constitutionally protected area: a suspect's home.[239] In *Kyllo*, the Court held that a Fourth Amendment search need not entail a physical intrusion; aiming a thermal imager at a house from a public street was sufficient to bring the police conduct within the scope of the Fourth Amendment.[240] Since the government, not the suspect, is initiating the transfer of information in these instances, the data would not be covered by the third-party doctrine.[241]

In contemporary society, physical contact is not needed to transfer information.[242] Whether the government needs to plug a cord into a medical device to download data or can accomplish the transfer wirelessly should not determine the scope of a suspect's Fourth Amendment protections.[243] In other words, a suspect's constitutional

237. *See* Wootson, *supra* note 5 (describing the investigator's tactics).

238. *See Grady*, 135 S. Ct. at 1370 (holding that a physical attachment is a search); *see also* United States v. Jones, 565 U.S. 400, 410 (2012) (ruling that the physical trespass constituted a search).

239. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (ruling that technology that allows officers to obtain information about activity inside a home is a search). Note the *Kyllo* Court decided that a Fourth Amendment violation had occurred based on the reasonable expectation of privacy theory, rather than the trespass theory. *See id.* at 34–35 (discussing *Katz* without any reference to physical trespass).

240. *See id.* (discussing why the officer's activity was a violation of privacy). The Court held that a search occurs when officers use "sense-enhancing technology" that is not in general public use to gain information not otherwise available to the public. *Id.* at 34.

241. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (noting that any information that individuals release to others is not protected by the Fourth amendment).

242. *See The Global Standard for Connection*, BLUETOOTH TECH., https://www.bluetooth.com/bluetooth-technology [https://perma.cc/82YP-LQGC] (last visited Mar. 11, 2019). AirDrop is another example of a product that allows users to wirelessly send data from one device to another. *See Use AirDrop on Your Mac*, APPLE SUPPORT, https://support.apple.com/en-us/HT203106 [https://perma.cc/7AZC-HCH2] (last visited Mar. 11, 2019) (discussing technology that allows Apple users to wirelessly share information with each other).

243. *See Kyllo*, 533 U.S. at 34 (emphasizing the flexibility of the privacy test). In *Kyllo*, officers used new technology to avoid a physical intrusion of the suspect's

protection should not hinge on a tangential design feature of his or her device.[244] To maintain consistency, the government should not be able to initiate the download of local data, either wirelessly or via physical intrusion, without a warrant or the suspect's consent.[245] Thus, wireless or physical access of local data on a suspect's medical device should receive Fourth Amendment protection under the physical intrusion theory.[246]

2. *Local Storage: Threshold Analysis Under the Privacy Theory*

The *Katz* decision laid out a two-prong privacy test to determine whether a search has occurred within the meaning of the Fourth Amendment: first, whether the person exhibited a subjective expectation of privacy, and second, whether that expectation is one that society is prepared to accept as reasonable.[247] Assuming that an individual exhibits an actual, subjective expectation of privacy regarding the data stored locally on his or her medical or health device, the analysis centers on whether his or her expectation of privacy is reasonable.[248] Health and medical data that is "shed" and then recorded

house, but the Court held that a Fourth Amendment search had still occurred. *See id.* at 34–35 (noting that a thermal imaging device that allowed officers to read heat signatures from a home was a search).

244. Rather, courts have looked to the quantity and quality of the data stored as determinative factors for Fourth Amendment protection. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (requiring a warrant to search a cell phone incident to arrest due to the quantity and quality of information stored in cell phones); State v. Worsham, 227 So. 3d 602, 604, 606 (Fla. Dist. Ct. App. 2017) (holding that "[a] car's black box is analogous to other electronic storage devices for which courts have recognized a reasonable expectation of privacy" because of the nature of the information contained within them).

245. *See, e.g.*, *Riley*, 134 S. Ct. at 2495 (requiring police to obtain a warrant before searching cell phones due to the highly personal data that is stored on them).

246. *See* Grady v. North Carolina, 135 S. Ct. 1368, 1371 (2015) (holding that remote GPS monitoring of a convicted sex offender constituted a search under the trespass theory).

247. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing the privacy theory test of whether a Fourth amendment search has occurred).

248. *Id.* ("[T]here is a twofold requirement, 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.'").

by a device on one's body shares similarities with urine collection and the collection of inadvertently shed DNA.[249]

In *Ferguson*, the Court held that obstetric patients have a reasonable expectation of privacy in the urine that they submit for drug screening, even though the urine is technically waste produced by the body.[250] Elsewhere, the Court has held that the collection of biological samples such as urine that do not involve any intrusion into the body are nonetheless searches because they intrude upon expectations of privacy related to medical information and the act of urination that "society is prepared to recognize as reasonable."[251] Thus, to the extent medical and health tracking devices record private biological data, the information recorded by these devices should be extended heightened Fourth Amendment protection.[252]

The Court has used the *Katz* privacy test to also analyze whether the warrantless collection of DNA constitutes a search under the Fourth Amendment.[253] While routine DNA collection is well established for convicted persons and arrestees, lower courts have been split on the constitutionality of collecting inadvertently shed DNA from individuals not under arrest.[254] In these circumstances, DNA may be collected from things like the seat of a suspect's chair, an inadvertently shed hair, or other biological material found on clothing in police custody.[255] Again, the shedding of DNA by the individual is inadvertent and thus is not a knowing exposure subject to the third-party doctrine.[256] Like skin cells or hair left behind on an interview chair, data about people's bodies is continuously "shed"

---

249. *See generally* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U.L. REV. 857 (2006) (describing how DNA is continuously discarded by the body).

250. Ferguson v. City of Charleston, 532 U.S. 67, 68, 76 (2001) ("[T]he urine tests conducted by those staff members were indisputably searches within the meaning of the Fourth Amendment.").

251. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 616 (1989).

252. *See id.* at 616–17 (explaining that urination is a private biological function protected by the Fourth Amendment).

253. *See supra* Subsection II.B.1 (describing applications of the *Katz* privacy test to urine collection and shed DNA).

254. *See, e.g.*, United States v. Davis, 690 F.3d 226, 251 (4th Cir. 2012); Raynor v. State, 99 A.3d 753, 754, 755 (Md. 2014); *see also* Angelique Romero, Comment, *Implications of* United States v. Jones *on DNA Collection from Arrestees: A Trespass Prohibited by the Fourth Amendment?*, 25 ST. THOMAS L. REV. 244, 245 (2013).

255. *See, e.g.*, *Davis*, 690 F.3d at 251; *Raynor*, 99 A.3d at 754.

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

throughout the day without their awareness.[257] Fourth Amendment scholar Andrew Guthrie Ferguson describes this shed data as a "data trail" that is created when an individual interacts with sensor surveillance throughout his or her day.[258] Once the medical and health devices begin recording, people are constantly shedding this data.[259]

Health and medical device data is also similar to DNA data in that both are inherently personal.[260] The Fourth Circuit in *Davis* emphasized the personal nature of DNA when ruling that Davis had a reasonable expectation of privacy in his DNA found on clothing that was lawfully in police custody.[261] The *Davis* Court contrasted the collection of DNA from clothing lawfully in police custody with the collection and analysis of paint chips found on clothing lawfully in police custody.[262] Unlike paint chips, individuals retain a reasonable expectation of privacy in their DNA, which can reveal "physiological data" and "a host of . . . medical facts."[263] It is precisely these privacy interests that are implicated in data held by medical and health tracking devices.[264] Like DNA, the data from these devices can reveal physiological information about one's health or wellbeing, such as whether someone is complying with medical treatment or the progression of a disease.[265]

The *Davis* decision contrasts with the decision in *Raynor*.[266] In *Raynor*, the Court of Appeals of Maryland held that the DNA testing of biological material left by a suspect on an interview chair was not

257. Dick Warrington, *Touch DNA*, FORENSIC MAG. (Dec. 27, 2010), https://www.forensicmag.com/article/2010/12/touch-dna [https://perma.cc/E8JC-3MZL] ("Because we are constantly shedding skin cells, when we touch something, we leave skin cells behind. Even if suspects leave only 6–8 skin cells from the outermost layer of their skin, scientists can use those cells to develop a DNA profile.").

258. *See* Ferguson, *supra* note 13, at 558–60. Ferguson develops a theory of "informational curtilage" to evaluate which data trails deserve Fourth Amendment protection. *See id.* at 619.

259. Joh, *supra* note 249, at 858 ("We leave traces—skin, saliva, hair, and blood—of our genetic identity nearly everywhere we go.").

260. *See id.* at 876–77 (describing the sensitive nature of DNA and medical information, particularly in connection with "behavioral genetics").

261. *See* United States v. Davis, 690 F.3d 226, 243 (4th Cir. 2012).

262. *See id.* at 244.

263. *Id.* at 243.

264. *See supra* Section I.B (detailing the medical facts collected by pacemakers, insulin pumps, Fitbits, and other devices).

265. *See* Appelboom et. al, *supra* note 20, at 3 (describing the physiological information made available by remote monitoring devices).

266. *See* Raynor v. State, 99 A.3d 753, 759 (Md. 2014).

a search within the meaning of the Fourth Amendment.[267] In so holding, the *Raynor* Court emphasized that the process used by law enforcement essentially turned the suspect's DNA into an identification number and did not reveal any intimate health or medical information.[268] In contrast, the data collected from medical devices is, by definition, associated with known medical or health conditions.[269] When police officers search medical and health devices for information, they are not merely trying to identify the subject, but rather they are trying to gain knowledge about that individual's activities, habits, or movements.[270] Therefore, the Maryland Court's reasoning for rejecting Raynor's argument does not apply in the case of medical and health device data.[271] For this reason, like the medical information stored within one's DNA, individuals have a reasonable expectation of privacy for medical and health data stored locally on their devices.[272] As such, this data should receive Fourth Amendment protections under the privacy theory.[273] Thus, a government search of locally stored medical or health data will implicate the Fourth Amendment whether the court's analysis is done under the trespass theory or the reasonable expectation of privacy theory.[274]

B. Is It a Search? The Threshold Question for Transmitted Data

Many health and medical tracking devices transmit the individual's locally stored data to a third-party hosting service.[275] Once

267. *See id.* at 82, 85 (holding that because police officers did not test regions of the DNA strand that carried "intimate genetic information," the DNA test was not a search within the meaning of the Fourth Amendment).

268. *See id.* at 86.

269. *See* Appelboom et. al, *supra* note 20, at 3 (describing clinical applications for medical and health tracking devices).

270. *See* Jackson, *supra* note 62 (describing ways in which law enforcement uses digital data in criminal investigations).

271. *See Raynor*, 99 A.3d at 761 (reasoning that Raynor had no reasonable expectation of privacy in his DNA because medically sensitive areas of his DNA were not tested).

272. *See* United States v. Davis, 690 F.3d 226, 243 (4th Cir. 2012); *see also* State v. Worsham, 227 So. 3d 602, 604 (Fla. Dist. Ct. App. 2017) (holding that car owners have a reasonable expectation of privacy in the personal driving data stored in their vehicle's "black box" or "event data recorder" and that a warrantless search of an impounded car's black box violated the Fourth Amendment).

273. *See Worsham*, 227 So. 3d at 604.

274. *See supra* Subsection III.A.1 (analyzing locally stored data using the *Jones* trespass theory).

275. *See* Bailey, *supra* note 29, at 889; *see also* FDA Safety Notice, *supra* note 31; *A Bluetooth-Enabled Pacemaker Provides Flexibility to Patients*, *supra* note 48;

the data is on the server, third parties, such as physicians, may access the data and view it in aggregate to identify patterns in activity or behavior.[276] The patient or user may initiate transmission manually, like when he or she opens the Fitbit application, or the data may be uploaded continuously throughout the day.[277] Traditionally, the Court has understood this type of data transmission to fall squarely within the third-party doctrine; however, recent arguments by Justice Gorsuch may show a way forward for a "data as property" view.[278]

1. *Transmitted Data: Threshold Analysis Under the Trespass Theory*

For a Fourth Amendment violation to occur under the trespass theory, the government must intrude upon a constitutionally protected area in order to gather information without a warrant or the party's consent.[279] Typically, these constitutionally protected areas have been understood as the areas outlined in the Fourth Amendment text itself: persons, houses, papers, and effects.[280] In other words, the areas in which the suspect has a property interest receive Fourth Amendment protection.[281] If, however, one's *data* could be construed as one's property, defendants could use the *Jones* trespass test to trigger Fourth Amendment protection.[282] Under this understanding, one's data, no matter where it is stored, receives Fourth Amendment protection under the property view.[283]

Justice Gorsuch raised this issue during oral arguments for *Carpenter v. United States*.[284] Justice Gorsuch inquired whether if a

---

FITBIT, *supra* note 49 (identifying how certain medical and health tracking data is transmitted to a third-party server).

276. *See, e.g.*, *A Bluetooth-Enabled Pacemaker Provides Flexibility to Patients*, *supra* note 48 (explaining the Bluetooth-enabled pacemaker provided by Cone Health Medical Group).

277. *See generally* FITBIT, *supra* note 49.

278. *See, e.g.*, United States v. Miller, 425 U.S. 435, 437 (1976) (holding the government acquisition of an individual's personal bank records does not constitute a search under the Fourth Amendment).

279. *See* United States v. Jones, 565 U.S. 400, 407 (2012).

280. *See, e.g.*, LAFAVRE, *supra* note 67, § 2.3. "Prior to the decision in *Katz v. United States*, the Supreme Court often used the concept of a 'constitutionally protected area' to define the reach of the Fourth Amendment's protections." *Id.*

281. *See id.* § 2.1(e).

282. *Jones*, 565 U.S. at 404–05 ("[T]he text of the Fourth Amendment reflects its close connection to property . . . .").

283. *See id.* at 404.

284. *See* Transcript of Oral Argument, *supra* note 206, at 38.

thief were to break into a T-Mobile store and steal consumer-location data, planning to profit from it, customers whose data was stolen would have a tort claim for conversion.[285] If so, and if consumers were recognized as having a property right in their data, a similar acquisition of consumer-location data by law enforcement would constitute a search under the property theory recognized in *Jones*.[286] During this exchange with Justice Gorsuch, government counsel argued that a property interest has never been recognized in information that is transferred to a business or a third party.[287] Justice Alito expressed support for the government's position.[288] In doing so, Justice Alito distinguished cell phone location data from property because the individual did not ask the cell phone company to create it, nor could the person force the cell phone company to destroy it.[289] Ultimately, Justices Alito, Thomas, and Gorsuch each authored a separate dissent to the *Carpenter* decision.[290] Justices Thomas and Gorsuch both argued that the Court should abandon the reasonable expectation of privacy test and the accompanying third-party doctrine in favor of a property-based approach.[291]

Federal statute does establish some rights to one's personal data for a cell phone consumer like Timothy Carpenter.[292] The Stored Communications Act of 1986 establishes privacy requirements for "customer proprietary [network] information."[293] Under that statute, a customer has the right to block or order the disclosure of his or her

285. *See id.* at 38, 52.

286. *See id.* at 52. Justice Gorsuch asked, "Wouldn't that, therefore, be a search of my paper or effect under the property-based approach approved and reminded us in *Jones*?" *Id.*; *see also* Mark Joseph Stern, *Neil Gorsuch's Independent Streak*, SLATE (Nov. 30, 2017, 2:52 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2017/11/in-carpenter-v-united-states-neil-gorsuch-showed-his-independent-streak.html [https://perma.cc/5NV3-LE2V].

287. Transcript of Oral Argument, *supra* note 206, at 55. Counsel for the United States argued that such a property right would "resemble no property right that's existed." *Id. But see* James Madison, *Property*, *reprinted in* 1 THE FOUNDERS' CONSTITUTION 598, 598 (Phillip B. Kurland & Ralph Lerner eds., 1987) ("In its larger and juster meaning, [property] embraces every thing to which a man may attach a value and have a right; and which leaves to every one else the like advantage.").

288. *See* Transcript of Oral Argument, *supra* note 206, at 55–56.

289. *See id.*

290. *See* Carpenter v. United States, 138 S. Ct. 2206, 2235 (Thomas, J., dissenting); *id.* at 2206 (Alito, J., dissenting); *id.* at 2261 (Gorsuch, J., dissenting).

291. *Id.* at 2235 (Thomas, J., dissenting) ("This case should not turn on 'whether' a search occurred. . . . It should turn, instead, on whose property was searched."); *see also id.* at 2261–72 (Gorsuch, J., dissenting).

292. *See, e.g.*, 47 U.S.C. § 222 (2012).

293. *See id.* § 222(c)(1).

digital records from a telecommunications company.[294] A defendant may argue that by passing the Stored Communications Act, Congress was beginning to recognize the intersection of consumers' property and privacy interests in the digital age.[295] Federal law provides protection for consumer records, but it extends greater protection for the contents of an individual's communication.[296] If the Court interprets these statutes as creating a customer proprietary interest in his or her digital data, then the Fourth Amendment will require a corollary protection from unreasonable searches and seizures of that data under the *Jones* property test.[297]

State tort laws also have recognized a proprietary interest in certain types of digital data, upholding conversion as a cause of action that applies to intangible property such as electronic records.[298] Under New York law, the types of property subject to conversion claims are tangible personal property and intangible property that bears a substantial similarity to tangible property, such as electronically stored information.[299] However, the laws of conversion in New York do not protect fully intangible "property," such as a business opportunity or the right to benefits under a contract.[300] Similarly, the United States District Court for the Northern District of Illinois has held that under Illinois law a satellite television company may have a conversion claim against an individual who used a satellite descrambler to intercept satellite television without the company's authorization.[301]

---

294. *Id.* § 222(c)(2) ("A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.").

295. In fact, Carpenter argued that, since it was last amended when only nine percent of Americans had cell phones, the Stored Communications Act provides little guidance on the issue of Fourth Amendment protections for cell site location data. Brief for Petitioner at 50, *Carpenter*, 138 S. Ct. 2206 (2017) (No. 16-402).

296. *See* Claudia G. Catalano, Annotation, *Prohibited Voluntary Disclosure Under Stored Communications Act*, 9 A.L.R. Fed. 3d Art. 6 (2016); *see also* 18 U.S.C. § 2702 (2012).

297. *See* Transcript of Oral Argument, *supra* note 206, at 56–57. Justice Gorsuch asked rhetorically, "[T]he government can acknowledge a property right but then strip it of any Fourth Amendment Protection. Is that the government's position?" *Id.*

298. *See* Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1277–78 (N.Y. 2007).

299. *See In re* Abreu, 527 B.R. 570, 587 (Bankr. E.D.N.Y. 2015).

300. *See id.*

301. *See* Directv, Inc. v. Ostrowski, 334 F. Supp. 2d 1058, 1064 (N.D. Ill. 2004).

The Seventh Circuit also remarked in dicta that there is no reason why intangible property might not be susceptible to conversion.[302]

Advancing the property theory of Fourth Amendment protection would require the Court to recognize a legally cognizable proprietary interest in the health and medical data that is created by people's bodies.[303] Personal health and medical data is analogous to the satellite television data at issue in *DIRECTV, Inc. v. Ostrowski*, in that the party with the proprietary interest *creates* the health and medical data.[304] Unlike cell phone location data, in which the cell phone company creates a record of the user's location based on which cell tower the user's phone "pings,"[305] informational content of health and medical data is created by the users themselves and exists before it is shared with a third party.[306] In other words, if one has a proprietary interest in the medical and health data that one's body creates, that proprietary interest may be recognized by the Fourth Amendment trespass theory.[307]

---

302. FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300, 305 (7th Cir. 1990) (quoting WILLIAM LLOYD PROSSER, *Chapter 3*, *in* PROSSER AND KEETON ON THE LAW OF TORTS 92 (1984)) ("[T]here is perhaps no very valid and essential reason why there might not be conversion of intangible property.") (internal quotation marks omitted); *see also* Laura D. Mruk, *WiFi Signals Capable of Conversion: The Case for Comprehensive Conversion in Illinois*, 28 N. ILL. U. L. REV. 347, 348 (2008) (arguing that using another individual's wireless internet signal meets the elements of conversion under Illinois law).

303. In other words, the Court would need to recognize the data from our bodies as a constitutionally protected area, not unlike it held the body itself to be a constitutionally protected area in *Grady v. North Carolina*. *See* 135 S. Ct. 1368, 1370 (2015).

304. *Directv, Inc*., 334 F. Supp. 2d at 1064 ("[F]or purposes of conversion, it is not the intent to steal or pilfer property that matters, but rather an intent to exercise a dominion or control over the goods which is in fact inconsistent with the plaintiff's rights.").

305. Amy Howe, *Justices to Tackle Cell Phone Data Case Next Term*, SCOTUSBLOG (June 5, 2017, 12:52 PM), http://www.scotusblog.com/2017/06/justices-tackle-cellphone-data-case-next-term [https://perma.cc/32BL-8BNT] ("[H]istorical cell-site records . . . . indicate the cell towers with which a cellphone connected while it was in use.").

306. For instance, the device automatically records a Fitbit user's sleep patterns; the data is generated by the user's heart rate and movements throughout the night, recorded on the Fitbit device, then wirelessly transmitted to the Fitbit app. *See How Do I Track My Sleep With My Fitbit Device?*, FITBIT, https://help.fitbit.com/articles/en_US/Help_article/1314 [https://perma.cc/7QR5-SYXK] (last visited Mar. 11, 2019).

307. This proprietary interest would be similar to the interest recognized by *Directv, Inc.*, 334 F. Supp. 2d at 1064.

2. *Transmitted Data: Threshold Analysis Under the Privacy Theory*

For an individual's data to receive Fourth Amendment protection under the *Katz* privacy theory, the individual must exhibit a subjective expectation of privacy; furthermore, this expectation must be one that society recognizes as reasonable.[308] The third-party doctrine, as applied in *United States v. Miller* and *Smith v. United States*, holds that when an individual reveals private information to a third party, he or she forfeits any Fourth Amendment protections to that data.[309] In other words, the Court has found it unreasonable to expect privacy after knowingly revealing one's information to a third party.[310]

At first glance, the knowing transmission of private health or medical data to a third party seems to fit squarely within the third-party doctrine.[311] However, the third-party doctrine has never been absolute.[312] Congress has acted statutorily to limit the application of the third-party doctrine, and the Court has also exempted certain types of information from the third-party doctrine.[313] For instance, in *Ferguson* the Court held that obstetric patients retain a reasonable expectation of privacy in the results of urine samples voluntarily submitted for testing, and hospital staff may not reveal the outcome of those tests to law enforcement without the patient's consent.[314]

More importantly, the Supreme Court's recent *Carpenter* decision applies the reasonable expectation of privacy doctrine to a new type of internet metadata, cell site location information.[315] In *Carpenter*, the Court held that the historical personal location information held by a consumer's cell phone service provider was not subject to the third-party doctrine, and therefore accessing the data

308. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

309. *See generally* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

310. *See Smith*, 442 U.S. at 743–44.

311. *See, e.g.*, *Miller*, 425 U.S. at 440 (holding that a bank customer has no protectable Fourth Amendment interest in bank records knowingly shared with her financial institution).

312. *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001) (holding that obstetric patients have a protectable Fourth Amendment interest in urine samples they knowingly gave to hospital staff for testing).

313. *See id.*; *see also* Thompson, *supra* note 172, at 23–25 (providing examples of congressional limitations on the third-party doctrine).

314. *See Ferguson*, 532 U.S. at 84.

315. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

constituted a Fourth Amendment search.[316] The Court emphasized the narrowness of the *Carpenter* decision, and it did not address other forms of personal internet metadata, such as health and medical information.[317] However, the reasoning the Court used to exempt cell site location information (CSLI) from the third-party doctrine would likely apply to personal health and medical data as well.[318] For instance, both CSLI and health or medical data create many data points throughout the day, giving law enforcement a unique window into the user's minute-to-minute routine.[319] In addition, just as cell phone use is a nearly indispensable part of modern life, health or medical devices may be recommended or required by the user's physician, meaning that the data is not voluntarily exposed in the same way personal banking data is voluntarily exposed to the user's bank.[320] In a forthcoming work that synthesizes the *Carpenter* reasoning, legal scholar Orin Kerr proposes that personal internet records should receive Fourth Amendment protection when (1) the collection of the information is only made possible by surveillance methods of the digital age, (2) the digital records are not the product of a user's meaningful voluntary choice, and (3) the records are of a type that tend to reveal an intimate portrait of a person's life.[321]

Arguing that the third-party doctrine should apply to health and medical data, the government may rely on case law upholding the third-party doctrine for credit or debit card data which tells where and when a user shops and the amount of his or her purchases.[322] This credit card transaction data, which can track the nature and amount of one's expenses, subscriptions, and location, is no more or less private than health and medical data, the government may argue.[323] However,

316. *See id.* at 2217. The *Carpenter* opinion limits its holding to the statement that accessing seven days of historical cell site location data constitutes a Fourth Amendment search. *See id.* at 2217 n.3.

317. *See id.* at 2220 ("Our decision today is a narrow one.").

318. *See id.* at 2216–19.

319. *See id.* at 2216 (describing CSLI as "detailed, encyclopedic, and effortlessly compiled").

320. *Id.* at 2220 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly 'shared' as one normally understands the term.").

321. *See* Orin S. Kerr, Implementing Carpenter 3 (Dec. 18, 2018) (unpublished manuscript).

322. *See, e.g.*, United States v. Dorsey, No. CR 14-328-CAS, 2015 WL 847395, at *18 (C.D. Cal. Feb. 23, 2015) (applying *Miller* to a defendant's recorded debit and credit card transactions).

323. Justice Alito raised this argument during the *Carpenter* oral arguments. *See* Transcript of Oral Argument, *supra* note 206, at 4–5.

personal medical and health data is distinguished from credit and debit card data in at least three ways. First, American society has demonstrated a heightened expectation of privacy related to medical and health information.[324] Second, the number of data points collected by a period of medical and health monitoring are often greater than the number of data points yielded by credit card information.[325] And finally, credit card transactions are more voluntary than medical devices, which some patients may rely upon to sustain their lives.[326]

In analyzing whether a search violates the Fourth Amendment, the Court must consider the social norms governing reasonable expectations of privacy.[327] The social norms around health and medical information indicate that American society has heightened expectations of privacy for this information.[328] One manifestation of this heightened expectation of privacy is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which created an offense for sharing individually identifiable health information with a third party.[329] Congress passed HIPAA with the goal of protecting patient privacy, and in the years following the passage of HIPAA, President Bill Clinton issued an executive order further protecting patient confidentiality in the course of government business.[330]

---

324. *See supra* Section I.C (describing American social norms surrounding personal medical and health information).

325. *See* FED. RESERVE SYS., THE FEDERAL RESERVE PAYMENTS STUDY 2016, 2–4 (2016), https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf [https://perma.cc/TFB5-KWLN] (discussing trends in consumer debit and credit card use and identifying the volume of data points collected by credit and debit card transactions each year in the United States).

326. *See generally* Stiles, *supra* note 30 (observing that pacemaker patients with remote monitoring have a greater likelihood of survival).

327. *See* Oliver v. United States, 466 U.S. 170, 178 (1984) (explaining that in each instance, the court must consider "our societal understanding that certain areas deserve the most scrupulous protection from government invasion").

328. *See supra* Section I.C (detailing programs such as HIPAA as evidence for heightened social norms protecting the privacy of health and medical information).

329. *See* 42 U.S.C. § 1320d-6 (2012).

330. *See* Health Coverage Availability and Affordability Act of 1996, H. R. Rep. No. 104-496, at 100 (1996) (stating in committee report that "[p]rotecting the privacy of individuals is paramount"); *see also* To Protect the Privacy of Protected Health Information in Oversight Investigations, 65 Fed. Reg. 81,321, 81,321 (Dec. 26, 2000) (stating that the government "may not use protected health information concerning an individual that is discovered during the course of health oversight activities for unrelated civil, administrative, or criminal investigations of a non-health oversight matter").

The American Medical Association's Code of Medical Ethics provides additional evidence of heightened social norms surrounding the privacy of medical and health information.[331] The Code describes patient privacy as a core health care value and essential to establishing trust in the patient–provider relationship.[332] Furthermore, rules of evidence that protect communications between a physician and patient, and the congressional defense of these rules, provide further evidence of such social norms.[333] Taken together, HIPAA, the American Medical Association's Code of Ethics, and the protections of patient–physician privilege illustrate that medical and health information are among the areas that deserve "the most scrupulous protection from government invasion."[334]

Personal health and medical data also differ from daily debit and credit card data in the number of data points recorded.[335] A Fitbit device records thousands of steps each day for the user, and an integrated GPS tracker can identify the user's location every minute of the day.[336] In contrast, debit card users conduct an average of 23.6 transactions per month.[337] So, although a record of debit card transactions may identify a user's location once or twice per day, the volume of location data recorded by debit cards is significantly less than the volume recorded by medical and health trackers.[338] In the past, the Court has looked to the volume of data collected to determine whether the Fourth Amendment may have been triggered, finding that the more data yielded by a government activity, the greater the likelihood that the government activity will be a search within the meaning of the Fourth Amendment.[339] Therefore, the quantity of data

331. *See* AM. MED. ASS'N, CODE OF MEDICAL ETHICS § 3.1.1 (2016)

332. *See id.*

333. Graham & Murphy, *supra* note 78, § 5521.

334. Oliver v. United States, 466 U.S. 170, 178 (1984).

335. *See supra* Section I.A (describing the volume of data collected by personal medical and health trackers).

336. *See* FITBIT, *supra* note 49.

337. Since the 2008 recession, debit card transactions have outpaced credit card transactions for daily consumer use. *See generally* FED. RESERVE SYS., *supra* note 325. In 2016, debit card issuer Pulse reported that the number of transactions per active card user reached 23.6 per month, a record high. *PULSE Study: Debit Fraud Loss Rates Decline After Chip Cards Introduced*, BUS. WIRE (Aug. 14, 2017, 2:50 PM) [hereinafter *PULSE Study*], https://www.businesswire.com/news/home/20170814005875/en/PULSE-Study-Debit-Fraud-Loss-Rates-Decline [https://perma.cc/8SUW-FP7U].

338. *See PULSE Study*, *supra* note 337.

339. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (holding that the government may not search a cell phone as part of a lawful search incident to arrest,

collected by health and medical devices distinguishes them from credit and debit card transactions, weighing in favor of exempting health and medical data from the third-party doctrine.[340]

Personal medical and health data is also distinguished by the degree of voluntariness with which some users employ the devices.[341] Typically, a consumer who wishes to keep a particular financial transaction private may, with minimal inconvenience, use cash or money order.[342] In contrast, some users of medical tracking devices rely on them for serious medical conditions.[343] For instance, Ross Compton, the Ohio man whose pacemaker data was used against him in an arson investigation, likely relied upon his pacemaker for lifesaving medical support.[344] Users who are told by their doctors that they need these devices for critical medical problems have their data recorded with far less voluntariness than a debit card user or even a cell phone user.[345] Thus, medical and health data is further distinguished from the financial data at issue in *Miller*.[346] Since medical and health data is significantly different than the information at issue in the classic third-party doctrine cases of *Smith* and *Miller*, the Court should carve out an exception to the third-party doctrine for medical and health information, just as it did with the obstetric patients' drug test results in *Ferguson*.[347]

---

and noting that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person"); United States v. Jones, 565 U.S. 400, 403 (2012) (noting that the GPS device placed on the defendant's vehicle "relayed more than 2,000 pages of data over the 4-week period").

340. *See* FITBIT, *supra* note 49 (describing the continual monitoring provided by the device); *PULSE Study*, *supra* note 337. (describing the average number of debit card transaction per user per month).

341. *See* Section I.A (describing how some medical device trackers are necessary to maintain a patient's health or wellbeing).

342. *See* Justin Pritchard, *Money Order Basics: Tips for Payments*, BALANCE, https://www.thebalance.com/money-order-basics-315432 [https://perma.cc/5ZSL-CLCX] (last updated Oct. 30, 2018).

343. *See* Stiles, *supra* note 30 (noting that pacemaker patients with high remote monitoring use had a fifty-three percent greater survival rate than patients with low remote monitoring use).

344. Ross Compton had numerous medical problems and was generally in poor health. *See* Johnson, *supra* note 2.

345. *See* Stiles, *supra* note 30.

346. *See* United States v. Miller, 425 U.S. 435, 439–40 (1976) (holding that bank customers did not have a reasonable expectation of privacy in records held by their financial institutions).

347. *See* Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001) (holding that urine samples obstetric patients knowingly gave to hospital staff for testing were exempt from the third-party doctrine).

CONCLUSION

Justice Scalia wrote in *Kyllo v. United States* that "in the sanctity of the home, all details are intimate details."[348] Similarly, within the sanctity of the human body, all details are intimate details.[349] It is precisely these details—such as the speed of one's heartbeat and the length of one's stride—that medical and health technologies capture and record.[350] The intimacy of these details and their value to law enforcement illustrate why the courts should afford this data Fourth Amendment protections.[351] When the data is stored locally on a device worn on or in the person's body, the Court should provide protections for this data that is coextensive with the protections provided to individual's bodies themselves, regardless of whether a physical intrusion is necessary to access the local data or whether it may be accessed wirelessly.[352] When the data is transmitted to a remote server for monitoring, the Court should carve out an exception to the third-party doctrine that protects the privacy of this data even when it is disclosed to a third party.[353] In so doing, the Court will align itself with the reasonable expectations of privacy for these devices and protect society's balance between safety and freedom.[354]

348. Kyllo v. United States, 533 U.S. 27, 28 (2001).

349. *See supra* Section I.C (detailing the social norms related to the privacy of personal health and medical information).

350. *See supra* Section I.A (describing the nature of the data collected by health and medical device trackers).

351. *See id.*; *see also supra* Section I.B (describing the value of medical and health data to both medical professionals and law enforcement).

352. *See supra* Section III.A (analyzing Fourth Amendment protections for locally stored data using both the trespass and privacy theories).

353. *See supra* Section III.B (analyzing Fourth Amendment protections for transmitted data using both the trespass and privacy theories).

354. *See* Oliver v. United States, 466 U.S. 170, 178 (holding that when determining the scope of Fourth Amendment protections, the courts must apply "our societal understanding that certain areas deserve the most scrupulous protection from government intrusion").