2024

Digital Rummaging

Andrew Guthrie Ferguson

DIGITAL RUMMAGING

ANDREW GUTHRIE FERGUSON*

ABSTRACT

The digital world encodes our lives with incriminating clues. How you travel, live, love, and shop are tracked through growing surveillance technologies. Police have recognized this reality and are actively exploiting new surveillance tools for investigative purposes.

The Fourth Amendment—the constitutional protection meant to limit police search powers—has not kept up with the privacy and security threats of these new digital technologies. Current doctrine has remained stymied by legal tests asking all the wrong questions about "reasonable expectations of privacy" and "trespass" searches. While the Supreme Court has acknowledged that "digital is different," it has not yet provided a coherent theory to protect individuals from growing digital surveillance.

This Article offers an alternative Fourth Amendment theory based on the harm of rummaging—a principle that can trace its lineage from the Founding debates around General Warrants and the Writs of Assistance to the Supreme Court's most recent cases on cell phone location data. Fear of government agents rummaging into private homes and papers motivated the passage of the Fourth Amendment and has remained a doctrinally coherent throughline recurring in Fourth Amendment cases.

This Article develops the "rummaging test" as a new way to see the harms of government collection of digital evidence. The Article excavates rummaging as an original justification for the Fourth Amendment and then demonstrates how the digital rummaging concept perfectly responds to the harms of government surveillance in the digital age. The rummaging test recognizes that the arbitrary, overbroad, invasive, exposing collection of personal data reflects the same harms that gave rise to the Fourth Amendment in the first instance.

The Article seeks to refocus attention on the government's power to rummage through personal data by examining legal challenges around smart-home data and long-term pole cameras. The hope is to move the longstanding background principle against rummaging to the foreground of Fourth Amendment analysis and thereby answer some of the hardest questions facing courts confronting challenges to digital surveillance.

---

* Professor of Law, American University Washington College of Law. Thank you to Professors Maneka Sinha, Kate Weisburd, Barry Friedman, Sonja Starr, Farah Peterson, Richard McAdams, Lior Strahilevitz, and Adam Davidson for helpful comments on this Article.

TABLE OF CONTENTS

INTRODUCTION

Clues to criminal investigation are now encoded in data. Smart cars, smartphones, smart homes, and smart payments track where we go, what we do, how we live, and what we spend.[1] While much of that activity is innocent, some is "criminal," and police have an incentive to uncover the

1. *See, e.g.*, Gabriel Bronshteyn, *Searching the Smart Home*, 72 STAN. L. REV. 455, 459 (2020) (discussing the home-tracking capabilities of a smart home); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 819–20 (2016) (discussing the rise of digital tracking sensors built in smart devices).

incriminating details. At the same time, the Fourth Amendment[2]—the constitutional protection that purportedly limits government overreach[3]—remains decidedly analog, still beholden to a world of physical searches and human intrusions.[4] The tension created by digital investigations is real: police know the digital clues exist, and yet, "we the people" want some measure of privacy and security from government surveillance.[5]

The questions arising from this tension have confounded courts. Take, for example, two recurring legal puzzles arising from digital police surveillance. First, can police acquire the smart data from a smart home that connects speakers, computers, refrigerators, and lights without a warrant?[6] Is there an expectation of privacy in smart-home data that has been shared with private third-party providers?[7] Second, should police be able to erect digital surveillance cameras around a home and monitor who comes in and out for over a year?[8] Do people have a reasonable expectation of privacy against long-term digital surveillance?[9]

The short answer is that the current Fourth Amendment offers little clarity—even though real cases raising those very questions are being litigated in courts today.[10] A focus on threshold questions of "searches" and "reasonable expectations of privacy" has created a muddled doctrine[11] that does not address larger-scale surveillance harms created by digital technologies. Something is missing from the legal analysis of these digital investigation cases that addresses the privacy and security harms of overbroad and unlimited governmental access to our lives.

---

2. U.S. CONST. amend. IV.

3. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 227 ("The Fourth Amendment is designed to safeguard individuals against governmental overreach.").

4. *See* Andrew Guthrie Ferguson, *Why Digital Policing Is Different*, 83 OHIO ST. L.J. 817, 824 (2022) (discussing the human involvement in using analog surveillance technology).

5. This Article focuses on the American criminal legal system with a particular focus on the Fourth Amendment and constitutional protections of privacy and security.

6. *See* Meagan Flynn, *Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over*, WASH. POST (Nov. 14, 2018, 7:28 AM), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/ [https://perma.cc/J8R8-4Y6W].

7. *See* Laurie Thomas Lee, *Smart Home Data Privacy and an Evolving Fourth Amendment*, 51 STETSON L. REV. 69, 70 (2021) (discussing smart homes and the third-party doctrine).

8. *See, e.g.*, United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022) (upholding the use of a long-term pole camera in operation for eighteen months).

9. *See* Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 50–53 (2022) (discussing expectations of privacy around digital pole cameras).

10. *See infra* notes 278, 280, 310, 312.

11. Criticisms of the *Katz* "reasonable expectation of privacy test" have long echoed among scholars. *See, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence."); *see also* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

This Article explains what is missing—the harm of rummaging. Rummaging is a distinct constitutional harm that has been minimized in the reasonable expectation of privacy analysis.[12] Yet rummaging and the prohibition against government agents indiscriminately acquiring personal information is not only central to the Fourth Amendment's history but serves as a vivid throughline in existing doctrine.[13] Rummaging—and the fear of government agents abusing their search powers—can be traced from the Founding debates around the Writs of Assistance and General Warrants to modern cases involving digital technologies.[14] In addition, the rummaging principle can be seen across a wide spectrum of Fourth Amendment cases—from warrant particularity to the plain view doctrine to the numerous other exceptions to the warrant requirement.[15] In fact, as this Article demonstrates, the rummaging principle offers a hidden logic that clarifies much of Fourth Amendment theory.

As will be detailed, my argument is that digital rummaging is a cognizable Fourth Amendment violation—a stand-alone harm that turns an overbroad government request for data into an unreasonable and thus unconstitutional act.[16] The act of rummaging invades the security interests protected by the Fourth Amendment and should be considered both a search and an unreasonable one. The anti-rummaging principle—described here as "the rummaging test"—can be applied in addition to the "reasonable expectation of privacy test"[17] or the "trespass test,"[18] providing a third threshold test to demarcate a police action as violative of the Fourth Amendment.[19] Rummaging also represents a substantive unreasonableness

12. *See infra* Part II.

13. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 72 ("Famous search and seizure cases leading up to the Fourth Amendment involved physical entries into homes, violent rummaging for incriminating items once inside, and then arrests and the taking away of evidence found. These examples, and some contemporaneous statements during the ratification debates, suggest that home entries and rummaging around inside were understood as the paradigmatic examples of 'searches.'"); Bronshteyn, *supra* note 1, at 457 ("Indeed, the image of the constable rummaging through private homes without permission or a warrant was the precise evil against which the Fourth Amendment's protections were drafted.").

14. Nicole Friess identified the harm of digital rummaging in the context of stored emails over a decade ago. *See* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 1010 (2012) ("A search for and seizure of stored e-mails and files should extend no further than necessary to find the particular communications the warrant describes. Requiring the government to provide the aforementioned level of detail protects privacy interests under the Fourth Amendment by preventing digital rummaging." (footnote omitted)).

15. *See infra* Part II.

16. *See infra* Part III (setting forth the rummaging principle).

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

18. *See* United States v. Jones, 565 U.S. 400, 409 (2012) (referring to a "common-law trespassory test").

19. The term "threshold test" is used to describe the threshold question of whether the Fourth Amendment applies. Under current doctrine, the Supreme Court first asks whether the Fourth

criterion that can be applied to digital surveillance even with a warrant. As will be discussed, this claim to "security" from government rummaging finds grounding in Founding Era documents and Fourth Amendment theory and is a normatively better response to the privacy threats of new digital surveillance technologies.[20]

The rummaging test poses a deceptively simple question: are police seeking otherwise secured information in an unparticularized or overbroad manner? If so, police are rummaging in violation of the Fourth Amendment, and the act is unreasonable and thus unconstitutional. Factors to determine whether a police agent is rummaging involve avoiding the harms that gave rise to the Fourth Amendment in the first place, namely: (1) avoiding *arbitrary* grants of generalized police power; (2) limiting *overreach* from initially justified searches; (3) protecting against *intrusion* of constitutionally protected interests (like the security of homes, papers, persons, and effects); and (4) minimizing *exposure* to embarrassing private information.[21] Each of these identified harms can claim root in decades of Supreme Court caselaw, and they collectively provide a framework to analyze the future challenges introduced by new digital surveillance technologies.

Part I of this Article explores the theme of rummaging in Fourth Amendment doctrine and history. Once identified as a stand-alone value, the concept can be seen reappearing in numerous Supreme Court cases. This Part looks at the general legal consensus around the harm of rummaging, its connection to early American history, and its direct and indirect influences on Fourth Amendment theory across a wide number of cases.[22] This Part also shows how the Supreme Court has largely adopted the rummaging theory in recent digital cases without acknowledging that reality. Part II then identifies the rummaging test as an analytical framework that can be used to determine an unreasonable governmental use of surveillance technology. As will be discussed, the rummaging principle crystalizes several harms that are currently undervalued in modern Fourth Amendment theory. Finally, Part III will apply the rummaging principle to the two open Fourth

---

Amendment applies by asking whether a search has occurred. The two controlling threshold tests are the "reasonable expectation of privacy test" and the "trespassory test." *See supra* notes 17–18. If there is no threshold search, there can be no Fourth Amendment violation.

20. *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 350–66 (1998) (describing the historical argument for why security as opposed to privacy is a better framework for analyzing Fourth Amendment protections). In prior work, I have argued for the term "security" to be used instead of "privacy." *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 614–16 (2017) (discussing informational security).

21. Each of these principles will be discussed in detail in Section II.A.

22. *See infra* Section I.C (discussing the theme of rummaging apparent in Fourth Amendment doctrine).

Amendment questions that began this paper focusing on (1) smart-home data and (2) long-term digital pole cameras. As will be demonstrated in Part III, the rummaging principle provides a relatively straightforward framework to analyze these otherwise difficult digital Fourth Amendment puzzles.

The goal of this Article is to refocus attention on the government's power to rummage through personal data. It is a necessary focus because the growth of digital surveillance technologies has outpaced Fourth Amendment theory that might otherwise limit that power.[23] The analysis—offered here—about digital rummaging offers an additional theory of Fourth Amendment protection at a time when police power to invade privacy has grown exponentially. It is also a theory that happens to be more consistent with the original understanding of the Fourth Amendment than current doctrine. The hope is, by moving the longstanding background principle against rummaging to the foreground of Fourth Amendment analysis, this Article can answer some of the hardest questions facing courts about digital surveillance.

I. RUMMAGING AND THE FOURTH AMENDMENT

The fear of government agents rummaging around homes, property, and papers animates much of Fourth Amendment theory.[24] The current Supreme Court—led by Chief Justice John Roberts—has repeatedly centered its understanding of the Fourth Amendment on the rummaging idea. For example, in *Riley v. California*[25]—a case involving the search of a smartphone incident to arrest—Chief Justice Roberts foregrounds his discussion about the Fourth Amendment by directly referencing the harm of police officers rummaging through private spaces: "Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to *rummage* through homes in an unrestrained search for evidence of criminal activity."[26]

23. Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 27 (2018) ("One aspect of why evaluating a modern reasonable expectation of privacy is so difficult is that technology has outpaced the applicability of the logic supporting many Fourth Amendment doctrines, creating the need for new rules that will uphold, rather than contravene, the privacy protections the Constitution is intended to confer.").

24. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 345 (2009) (recognizing that "the central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects").

25. 573 U.S. 373 (2014).

26. *Id.* at 403 (emphasis added).

In *Carpenter v. United States*[27]—a case involving cell-site location tracking—Chief Justice Roberts again quotes this same "rummaging" language linking the harm of British officers arbitrarily rummaging through homes as a motivating force for American independence.[28]

While disagreeing with the Chief Justice about the outcome of the case, Justice Samuel Alito in his *Carpenter* dissent nevertheless did agree with the Founding generation's concern about governmental rummaging into private matters.[29]

> General warrants and writs of assistance were noxious not because they allowed the Government to acquire evidence in criminal investigations, but because of the *means* by which they permitted the Government to acquire that evidence. Then, as today, searches could be quite invasive. . . . Private area after private area becomes exposed to the officers' eyes as they *rummage* through the owner's property in their hunt for the object or objects of the search. If they are searching for documents, officers may additionally have to rifle through many other papers—potentially filled with the most intimate details of a person's thoughts and life—before they find the specific information they are seeking.[30]

This recognition that privacy-invasive rummaging is directly connected to Fourth Amendment core principles has served as a point of consensus among judges and scholars.[31] As will be discussed, the language of rummaging recurs in many seminal Fourth Amendment cases,[32] so it is no accident that the harm of rummaging has emerged in digital cases like *Riley* and *Carpenter*.[33] As will be used here, the term "rummaging" encompasses government agents exploring in a limitless and generalized manner some

27. 585 U.S. 296 (2018).

28. *See id.* at 303–04 ("In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was 'the first act of opposition to the arbitrary claims of Great Britain' and helped spark the Revolution itself." (quoting *Riley*, 573 U.S. at 403)).

29. *See id.* at 369–70 (Alito, J., dissenting).

30. *Id.* (second emphasis added).

31. *See* Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 316–17 (2016) ("It has long been a common consensus that the Fourth Amendment guards against the evil of arbitrary government rummaging in people's lives.").

32. *See, e.g.*, Chimel v. California, 395 U.S. 752, 767–68 (1969) (discussing rummaging and search incident to arrest); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (discussing rummaging and plain view); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (discussing rummaging and warrant particularity); Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) (discussing rummaging and frisks); Florida v. Wells, 495 U.S. 1, 4 (1990) (discussing rummaging and inventory searches).

33. *See infra* Sections I.A–C (detailing the numerous examples of the use of "rummaging" in Fourth Amendment cases).

personal or private space, structure, or thing and the information contained in those areas, places, papers, and things.

The next few Sections give context and color to this admittedly broad definition of rummaging. The goal in these Sections is to highlight the historical and doctrinal role of the rummaging principle in Fourth Amendment law and theory. What will become clear is that, while rummaging has long been used as a limiting principle for warrants and searches with probable cause, the same logic can also apply across all Fourth Amendment questions, including threshold search questions. In fact, when applied to the threshold search question cases described in Section I.B, the addition of the rummaging principle adds doctrinal clarity especially in an age of pervasive data collection.

A. The Role of Rummaging in Fourth Amendment History

Rummaging as a word, as a harm, and as a fear can be found mentioned throughout early American history.[34] The Founding generation experienced the seismic harms of rummaging as a direct result of the heavy-handed actions of British agents investigating colonial rule breakers.[35] The Supreme Court has remained faithful to that history by referencing the stories and cases that first highlighted that original fear of arbitrary governmental power.[36]

1. The English Background

The consensus rejection of rummaging traces its influence to a few early English cases that had an outsized impact on the Founding generation.[37] Two of these cases—*Wilkes v. Wood*[38] and *Entick v. Carrington*[39]—have been well-examined by legal historians and Fourth Amendment scholars as canonical examples of the type of arbitrary power that sparked the American

34. *See* Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 IOWA L. REV. 1643, 1653 (2020) ("[R]ummaging through papers for new crimes is the very definition, for both the founding generation and contemporary courts, of the fishing expedition the Fourth Amendment (and likely Fifth Amendment) sought to prevent." (footnotes omitted)).

35. *See* United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013) ("The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of "general warrants."'" (quoting Payton v. New York, 445 U.S. 573, 583 (1980))).

36. *See* Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 918 (1985) ("The Supreme Court, mindful of the history of abuses in the background of the fourth amendment, has cautioned that the amendment's search and seizure clause does not permit an 'indiscriminate rummaging' or 'a general, exploratory rummaging' through an individual's possessions." (footnotes omitted)).

37. *See* Kerr, *supra* note 13, at 72.

38. (1763) 98 Eng. Rep. 489 (KB).

39. (1765) 95 Eng. Rep. 807 (KB).

Revolution and inspired the drafting of the Fourth Amendment.[40] The focus here will be on the specific role "rummaging" played as part of the articulated harm of these governmental practices.

Wilkes v. Wood involved the search of the home of John Wilkes—not only a member of Parliament but also the author of a publication called *The North Briton* that took critical aim at King George III.[41] Lord Halifax, then the Secretary of State, issued a warrant to search through Wilkes's home and papers to find evidence that he was the author of a particular edition of *The North Briton* that harshly criticized the King.[42] Agents of the Crown ransacked Wilkes's home, seized his papers, and invaded his private office. Wilkes sued the agents under a quasi-trespass theory, claiming that the warrant for his papers was unlawful and the search unreasonable.[43] In a decision that echoed across Britain and the American colonies, the court awarded Wilkes damages against the Secretary of State for the overbroad search of his papers and things.[44] The *Wilkes* court described the harm done:

> [T]hey *rummaged* all the papers together they could find, in and about the room . . . [T]hey (the messengers) fetched a sack, and filled it with papers. . . . Blackmore then went down stairs, and fetched a smith to open the locks. . . . [A] messenger, then came, and would whisper Mr. Wood, who bade him speak out; he then said he brought orders from Lord Halifax to seize all manuscripts.[45]

The identified privacy and liberty violations were not just about the actual physical papers or personal property seized but more the informational harm of a search power that could be abused by the government. The court recognized "[t]hat some papers, quite innocent in themselves, might, by the slightest alteration, be converted to criminal action."[46] The fear was that, by allowing rummaging into private papers,

40. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1196 (2016) ("Three influential cases laid the groundwork for the Founders' rejection of general warrants: *Entick v Carrington* in 1765, *Wilkes v Wood* in 1763, and *Leach v Money* in 1765." (footnotes omitted)); *see also* Orin S. Kerr, Katz *as Originalism*, 71 DUKE L.J. 1047, 1064 (2022); Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 255 (2019).

41. *See* Stanford v. Texas, 379 U.S. 476, 483–84 (1965) ("The *Wilkes* case arose out of the Crown's attempt to stifle a publication called The North Briton, anonymously published by John Wilkes, then a member of Parliament—particularly issue No. 45 of that journal.").

42. *Id.* ("Lord Halifax, as Secretary of State, issued a warrant ordering four of the King's messengers 'to make strict and diligent search for the authors, printers, and publishers of a seditious and treasonable paper, entitled, The North Briton, No. 45, . . . and them, or any of them, having found, to apprehend and seize, together with their papers.'").

43. *See Wilkes*, 98 Eng. Rep. at 489–90.

44. *Stanford*, 379 U.S. at 483–84 ("Holding that this was 'a ridiculous warrant against the whole English nation,' the Court of Common Pleas awarded Wilkes damages against the Secretary of State.").

45. *Wilkes*, 98 Eng. Rep. at 491 (emphasis added).

46. *Id.* at 490.

homes, and thereby personal thoughts, prosecuting officials could find incriminating materials that they did not even know existed against disfavored individuals, thus expanding suspicion beyond the original justification. In addition, of course, just the threat of this type of government search power created chilling effects on a person's thoughts, political views, and freedom to speak.

Similarly, another celebrated case, *Entick v. Carrington*, involved a search of private papers to confirm the authorship of a different statement of seditious libel against the King.[47] John Entick authored the offending publication and had his home searched and books and papers seized under the authority of a broadly written warrant.[48] Entick sued the offending agents under a quasi-trespass theory and won. The presiding judge, Lord Camden,[49] wrote a powerful legal opinion about the harms of searching private papers and homes and the corresponding values of protecting personal property and liberty. The United States Supreme Court has referenced *Entick* in several modern opinions[50] addressing the harm of rummaging through private spaces looking for possible evidence:

> In an opinion which this [Supreme] Court has characterized as a wellspring of the rights now protected by the Fourth Amendment, Lord Camden declared the warrant to be unlawful. "This power," he said, "so assumed by the secretary of state is an execution upon all the party's papers, in the first instance. His house is rifled; his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent

47. *See* Entick v. Carrington (1765) 95 Eng. Rep. 807, 817–18 (KB) ("[F]or papers are often the dearest property a man can have.").

48. *Stanford*, 379 U.S. at 483–84 ("John Entick was the author of a publication called Monitor or British Freeholder. A warrant was issued specifically naming him and that publication, and authorizing his arrest for seditious libel and the seizure of his 'books and papers.' The King's messengers executing the warrant ransacked Entick's home for four hours and carted away quantities of his books and papers.").

49. Lord Camden was Charles Pratt, 1st Earl of Camden.

50. *See, e.g.*, United States v. Jones, 565 U.S. 400, 405 (2012) ("*Entick v. Carrington* is a 'case we have described as a "monument of English freedom" "undoubtedly familiar" to "every American statesman" at the time the Constitution was adopted, and considered to be "the true and ultimate expression of constitutional law"' with regard to search and seizure." (citation omitted) (quoting Brower v. County of Inyo, 489 U.S. 593, 596 (1989))); Boyd v. United States, 116 U.S. 616, 626–27 (1886) ("As every American statesmen, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom, [*Entick*,] and considered it as the true and ultimate expression of constitutional law, it may be confidently asserted that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures."); Schnapper, *supra* note 36, at 870 ("Noting that the historical limitations on searches and seizures in England arose out of conflicts between the government and the press, the Court further insisted that any search warrant or subpoena for documents that affects free speech be scrutinized with particular care." (footnote omitted)).

> jurisdiction, and before he is convicted either of writing, publishing, or being concerned in the paper."[51]

Entick and *Wilkes* are understood to be cases that privileged the sanctity of personal papers and personal expression over government need for criminal evidence.[52] In both cases, the offending material was, in fact, criminal under existing laws.[53] In both cases, the agents had a signed judicial warrant authorizing the search and seizure. But, in both cases, the English courts rejected the idea that the government should have the power to root around a private space and discover offending papers (even treasonous ones).[54]

2. The American Colonial Experience

These early English cases provide the legal backdrop of the rejection of British search practices in the American colonies. Specifically, the colonists objected to the powers granted by General Warrants[55] and the Writs of Assistance.[56] Such overbroad grants of investigatory power led to overzealous enforcement in the colonies and provided fodder for American revolutionaries to complain about a specific sort of rummaging.

As has been mentioned, these rummaging powers directly influenced founding debates about government power and the Fourth Amendment.[57] For example, James Otis in his famous *Against Writs of Assistance* speech in Boston complained that the Writs allowed officers to enter houses, break

---

51. *Stanford*, 379 U.S. at 484 (footnote omitted).

52. In an excellent Article, Professor Laura Donohue has examined the early legal influences of *Entick*, *Wilkes*, and also *Purnell's Case* which involved an English court rejecting a request for incriminating documents. *See* Donohue, *supra* note 40, at 1310.

53. It is important to remember that the Fourth Amendment was designed to protect admittedly criminal behavior (sedition, tax avoidance, etc.) even in the face of legally sanctioned police investigation.

54. Schnapper, *supra* note 36, at 874 ("[T]he *Entick* court invalidated the seizure not because the court regarded the underlying warrant as a general warrant, but because the seizure violated the distinct prohibition on seizures of papers.").

55. Maryland v. King, 569 U.S. 435, 466 (2013) (Scalia, J., dissenting) ("At the time of the founding, Americans despised the British use of so-called 'general warrants'—warrants not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application.").

56. *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 219–20 (1993) ("The warrantless searches executed by British customs officers in the early 1750's, 'under which customs officers assumed a power of forcible entry *ex officio* and which had been resisted physically or contested at law,' led to the landmark Writs of Assistance Case of 1761. Customs officers, acting without warrants or other judicial authorization, forcibly entered private dwellings and warehouses looking for smuggled goods. Customs officials claimed that their authority for these warrantless searches derived from their commissions or deputations." (footnotes omitted)).

57. *See supra* notes 35–37.

locks, and invade the sanctity of the home.[58] Similarly, Patrick Henry raised the alarm about government agents who would "go into cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear."[59] George Mason also raised a concern about government agents who "will carry the exciseman to every farmer's house who distills a little brandy, where he may search and ransack as he pleases."[60] The fear in speeches, pamphlets, and rhetoric was the invasion of private lives by government agents using arbitrary and overbroad means to rummage for suspected incriminating evidence.

After American Independence and the ratification of the United States Constitution, advocates for a Bill of Rights continued to discuss the dangers of rummaging in an effort to rally the country toward ratifying the Fourth Amendment.[61] For example, as Professor Laura Donohue has catalogued in her extensive research into Fourth Amendment history, Anti-Federalist pamphleteers writing under the names "Father of Candor," "Son of Liberty," and a "Farmer and a Planter" all expressed concerns that government officials could "ravage," "expose," "seize private papers," and "rummage your houses from bottom to top."[62] The harms involved the

58. James Otis, Against Writs of Assistance (Feb. 24, 1761) ("Now, one of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege. Custom-house officers may enter our houses when they please; we are commanded to permit their entry. Their menial servants may enter, may break locks, bars, and everything in their way; and whether they break through malice or revenge, no man, no court can inquire. Bare suspicion without oath is sufficient.").

59. George C. Thomas III, *Stumbling Toward History: The Framers' Search and Seizure World*, 43 TEX. TECH L. REV. 199, 207 (2010) (citing 3 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION AS RECOMMENDED BY THE GENERAL CONVENTION AT PHILADELPHIA IN 1787, at 448–49 (Jonathan Elliot ed., Philadelphia, J.B. Lippincott Co., 2d ed. 1836) (Patrick Henry, June 14, 1788, the Virginia ratification convention)).

60. Thomas, *supra* note 59, at 207 (citing THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION AS RECOMMENDED BY THE GENERAL CONVENTION AT PHILADELPHIA IN 1787, *supra* note 59, at 209 (George Mason, June 11, 1788, Virginia ratification convention)).

61. *See* Maclin, *supra* note 56, at 227 ("Considering the history surrounding the writs of assistance, it is difficult to conclude that most colonial judges were insensitive to civil liberties, or anxious to expand the search powers of governmental officials. Rather, this evidence indicates that many judges, along with other colonists and colonial juries, strongly opposed practices that granted custom officers the discretion to invade the privacy and personal security of individuals." (footnotes omitted)).

62. *See* Donohue, *supra* note 40, at 1237–38 ("Underlying these rules was the importance of the sanctity of the home. As Almon, writing as the Father of Candor, eloquently explained in 1765: 'Nothing, as I apprehend, can be forcibly taken from any man, or his house entered, without some specific charge upon oath. The mansion of every man being his castle, no general search-warrant is good. It must either be sworn that I have certain stolen goods, or such a particular thing that is criminal in itself, in my custody, before any magistrate is authorized to grant a warrant to any man to enter my house and seize it. Nay further, if a positive oath be made, and such a particular warrant be issued, it can only be executed upon the paper or thing sworn to and specified, and in the presence of the owner, or of somebody intrusted by him, with the custody of it. Without these limitations, there is no liberty or free

manner in which private information was obtained by police looking for incriminating evidence.[63] The rummaging harm also touched on the nature of what could be exposed by this government intrusion, with a special emphasis on the information arising from personal papers.[64]

This Founding era history, thus, suggests a strong claim that the Fourth Amendment was influenced by a fear of law enforcement rummaging. In fact, I would argue that rummaging can make an equal historical claim to "trespass" in interpretive battles over the meaning of the Fourth Amendment right to be secure from unreasonable searches and seizures. At a minimum, the Fourth Amendment was designed to thwart government rummaging into private, secure places containing personal information.

3. Boyd v. United States

With this historical background, it is thus little wonder then that in 1886 when the Supreme Court was first tasked with interpreting the Fourth Amendment that the Justices went back to this early discussion of rummaging.[65] *Boyd v. United States* involved the government use of a court order to demand business records (invoices) in a criminal case investigating tax evasion.[66] The government sought evidence demonstrating a discrepancy in the amount of goods sold and taxes paid.[67] *Boyd* was not a major case involving sedition, political speech, or papers with personal

enjoyment of person or property, but every part of a man's most valuable possessions and privacies, is liable to the ravage, inroad and inspection of suspicious ministers, who may at any time harass, insult and expose, and perhaps, undo him.'"); *id.* at 1288 ("Writing in the *New-York Journal* in November 1787, a 'Son of Liberty' outlined 'a *few* of the *curses* which will be entailed on the people of America, by this preposterous and newfangled system, if they are ever so infatuated as to receive it.' The fourth item in the list read: 'Men of all ranks and conditions, subject to have their houses searched by officers, acting under the sanction of *general warrants*, their private papers seized, and themselves dragged to prison, under various pretences, whenever the fear of their lordly masters shall suggest, that they are plotting mischief against their arbitrary conduct.'" (footnote omitted)); *id.* at 1290–91 ("'A Farmer and Planter,' [was] an Anti-Federalist writing under a pen name, who published his objections in the *Maryland Journal*. 'The excise-officers have power to enter your houses at all times, by night or day, and if you refuse them entrance, they can, under pretence of searching for exciseable goods, . . . break open your doors, chests, trunks, desks, boxes, and rummage your houses from bottom to top.'").

63. *See* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 70–71 (2013) (detailing the role of advocates like the Father of Candor who had a significant impact on the political leaders of a young America).

64. *See* Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. C.R.-C.L. L. REV. 461, 463 (1981) ("Protection of private papers from governmental search and seizure is a principle that was recognized in England well before our Constitution was framed.").

65. *See* Donald A. Dripps, *Responding to the Challenges of Contextual Change and Legal Dynamism in Interpreting the Fourth Amendment*, 81 MISS. L.J. 1085, 1092 (2012) ("*Boyd* read the English decision in *Entick v. Carrington* to prohibit the seizure of private papers for evidentiary use, even if the seizure was authorized by a specific warrant.").

66. Boyd v. United States, 116 U.S. 616, 618 (1886).

67. *Id.*

meaning or significance. In fact, the business records at issue were quite ordinary and likely the type of documents that would be central in many tax avoidance prosecutions.[68] Further, the method of obtaining the papers did not require a physical search, violence, or even officers entering a home—the government merely asked for the records. Yet, relying on the types of searches condemned in *Entick* and *Wilkes*, the *Boyd* Court held that the government's demand for information violated the Fourth and Fifth Amendments.[69] In language that specifically referenced *Entick* and protecting the privacies of life against governmental rummaging, the Court wrote:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach further than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence,—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of that judgment. In this regard the Fourth and Fifth amendments run almost into each other.
>
> Can we doubt that when the Fourth and Fifth Amendments to the Constitution of the United States were penned and adopted, the language of Lord Camden was relied on as expressing the true doctrine on the subject of searches and seizures, and as furnishing the true *criteria* of the reasonable and "unreasonable" character of such seizures? . . . The struggles against arbitrary power in which they had been engaged for more than twenty years, would have been too deeply engraved in their memories to have allowed them to approve of such insidious disguises of the old grievance which they had so deeply abhorred.[70]

68. *See id.* (describing the invoice at issue).
69. *Id.* at 634–35.
70. *Id.* at 630 (emphasis added).

Two points are most relevant here. First, the *Boyd* Court explicitly referenced rummaging harms, inferring that the harm involves four related impacts: (1) the intrusion into private spaces; (2) an overbroad search power; (3) an arbitrary search power; and (4) the potential exposure of embarrassing information. These kinds of harms arising from government rummaging powers will be addressed throughout this Article.

Second, while the scope of *Boyd* has been dramatically narrowed by subsequent Supreme Court decisions which rejected the "mere evidence doctrine"[71] and largely ignored the Fifth Amendment aspects of Fourth Amendment claims,[72] the case itself is still cited for these rummaging harms. As will be discussed in detail later, Justices in *Jones v. United States* (2012), *California v. Riley* (2014), and *Carpenter v. United States* (2018) directly referenced *Boyd* to highlight the harm of arbitrary or intrusive police practices.[73] In fact, for a case that has arguably been repudiated in practice, *Boyd*'s spirit remains quite strong in modern Fourth Amendment theory.

4. Conclusion on the Early History of Rummaging

Colonial-era cases and the Supreme Court's embrace of the rummaging principle in *Boyd* reveal how the rummaging principle shaped an original understanding of the Fourth Amendment. Examined carefully, the original rummaging principle really has two related but distinct parts. First, there was a prohibition on arbitrary and overbroad investigatory powers, namely restricting the ability to search multiple places, people, or papers without individualized suspicion. Second there was a prohibition on general, exploratory searching within private areas, papers, and personal information even with particularized suspicion of a crime.

These two related principles have been conflated over time, but they are important to keep distinct. The first involved police power, and the second involved the protection of private papers, effects, and personal activities. As Professor Donald Dripps has recognized, the Writs of Assistance were reviled because government agents were given wide and unlimited powers

71. *See* Bradley, *supra* note 64, at 461 ("Until 1967 the mere evidence rule limited the objects of searches and seizures to 'fruits and instrumentalities' of a crime. This rule provided special, if illogical and arbitrary, constitutional protection to private papers, as they were rarely fruits or instrumentalities of crime. But in 1967, in *Warden v. Hayden*, the Supreme Court decided that the fourth amendment permitted searches for 'mere evidence.'" (footnotes omitted)).

72. *Boyd* suggests a more interrelated relationship between the Fourth and Fifth Amendments, protecting incriminating evidence that is obtained from the suspect themselves. *See Boyd*, 116 U.S. at 634–35.

73. United States v. Jones, 565 U.S. 400, 404–05 (2012); Riley v. California, 573 U.S. 373, 403 (2014); Carpenter v. United States, 585 U.S. 296, 305 (2018).

to search and surveil anyone.[74] The Writs did not authorize the seizures of papers but focused on the invasive potential of governments to rummage in the lives of the colonists (primarily their homes and businesses).[75] Separately, the General Warrants were reviled because they allowed the seizure of papers including papers libeling the King or otherwise dissenting against the British government. The decision to include "papers" in the Fourth Amendment is understood to protect against the rummaging of private materials once allowed by General Warrants.[76] This protection of personal information was broad, forbidding the act of looking through papers in the hopes of uncovering additional incriminating evidence.

As will be discussed in the next few Sections, these two anti-rummaging principles find new life in modern digital surveillance cases. For example, many of the cases finding a violation of a reasonable expectation of privacy turn on the arbitrary and overbroad nature of the police action—mirroring the fear of the Writs of Assistance that granted unchecked search powers to government actors.[77] Digital surveillance can be overbroad, vacuuming up data indiscriminately to be sorted through later for particular clues. Similarly, many of the cases finding an unreasonable search—even with particularized suspicion—turn on the fear that the search opens the door to rummaging into extraneous incriminating personal information—similar to the fear of the General Warrants.[78] These cases will be discussed in the next two Sections.

B. The Role of Rummaging in Fourth Amendment Doctrine

As has been demonstrated, the historical record evidencing a fear of rummaging is quite strong. How that fear has been operationalized in cases and Fourth Amendment theory, however, is a bit more nuanced. This Section contrasts two different manifestations of the rummaging principle

74. Dripps, *supra* note 63, at 61 ("The Fourth Amendment is generally seen as a response to two protests against particular abuses, the first against Writs of Assistance in the colonies in 1761–1762 and the second against general warrants in England in 1764–1765.").

75. *Id.* ("The inspiration for singling out 'papers' in the Fourth Amendment lies in this later controversy. John Adams's report of Otis's famous argument against the Writs of Assistance makes no special mention of papers. This is not surprising because the writs did not authorize seizure of papers, only of undutied goods. The English courts had not yet prohibited general warrants to search for and seize libels." (footnotes omitted)).

76. *Id.*

77. *Carpenter v. United States* and the search of CSLI is a good example of a technology that collects too much information about too many people to be left without a warrant requirement. *See Carpenter*, 585 U.S. at 312.

78. *Riley v. California* and the search of a smartphone is a good example of the limits required even when there is suspicion of a particular person or thing. In *Riley*, police had good reason to suspect David Riley of criminal involvement, but even that suspicion was not sufficient, in itself, to obviate a warrant requirement for additional data in the smartphone. *See* Riley, 573 U.S. at 403.

in modern Fourth Amendment cases. First, this Section shows how anti-rummaging logic has been built within the "reasonableness" doctrine. The following Section then shows how this same logic has been omitted in traditional "reasonable expectation of privacy" search analysis but has started to reemerge in more recent digital surveillance cases.

This first Section examines rummaging and reasonableness.[79] More specifically, it looks at how rummaging exists as a limiting principle to the scope of a search (even with particularized suspicion). The Supreme Court has explicitly referenced rummaging as an operating principle to limit searches beyond the initial place or source of suspicion.[80] In these cases, police generally have particularized suspicion of a place or person but go too far in looking for other evidence of other crimes.[81] Rummaging as an explicit limiting principle arises across a broad spectrum of Fourth Amendment cases involving search incident to arrest,[82] physical searches of homes and persons,[83] special needs searches,[84] and, of course, in the particularity of warrants.[85] In short, a concern about rummaging acts as a limiting principle on police power (even with particularized suspicion).

The next Section looks at rummaging and reasonable expectations of privacy.[86] Generally speaking, rummaging has been ignored in the threshold search discussion of whether the Fourth Amendment applies.[87] Asking whether an individual has a reasonable expectation of privacy is different than asking if the government used a particular power to rummage through something private. In ignoring the rummaging principle (in its threshold discussions), the Supreme Court has allowed literal rummaging in trash without finding the police action a Fourth Amendment "search" let alone an unreasonable one.[88] Yet, recent cases involving digital technologies have forced the Court to rethink the rummaging harms in overbroad surveillance.[89]

---

79. Reasonableness is central to Fourth Amendment analysis. *See, e.g.*, Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness.").

80. *See* Warden v. Hayden, 387 U.S. 294, 320–21 (1967) (Douglas, J., dissenting).

81. *See* Arizona v. Gant, 556 U.S. 332, 344–45 (2009).

82. *See* Chimel v. California, 395 U.S. 752, 767–68 (1969) (search incident to arrest).

83. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (plain view); Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) (plain feel).

84. *See* Florida v. Wells, 495 U.S. 1, 4 (1990) (inventory searches).

85. *See* Andresen v. Maryland, 427 U.S. 463, 480 (1976) (particularity).

86. The reasonable expectation of privacy test comes from Justice Harlan's concurrence in *Katz v. United States* and remains one of the controlling threshold tests of whether a Fourth Amendment "search" has occurred. *See* Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).

87. *See infra* Section I.B.2.

88. *See* California v. Greenwood, 486 U.S. 35, 40 (1988). *Greenwood* is discussed in detail Part II.

89. As discussed at the beginning of Part I, both *Carpenter v. United States*, 585 U.S. 296 (2018), and *Riley v. California*, 573 U.S. 373 (2014), begin with a discussion of the harms of rummaging.

In fact, as I will argue, the shift to digital surveillance necessitates this recognition of rummaging harms. As will be discussed, one of the realities of early Fourth Amendment search cases was that most involved rather low-tech surveillance tools with minimal surveillance capacity.[90] Whether it was the tape recorder in *Katz*,[91] the plane flight in *California v. Ciraolo*,[92] or the beeper in *United States v. Knotts*,[93] the technologies were not sophisticated enough to raise rummaging concerns.[94] This has started to change with new twenty-first century technologies which now allow for overbroad collection of data against many people and for long periods of time.[95] Once audio sensors can listen to entire neighborhoods,[96] planes can videotape entire cities,[97] or smartphone apps can track all users all at once,[98] the old logic of analog cases falls away. In fact, in cases like *Carpenter* and *Jones*, the rummaging harm has reemerged as a helpful organizing principle.[99]

Studying these two distinct lines of Fourth Amendment cases leads to one conclusion—namely that incorporating the rummaging principle into both reasonableness and the threshold search analysis will clarify the doctrine and help solve some of the harder puzzles of digital surveillance.

---

90. *See* Ferguson, *supra* note 4, at 824.

91. *See* Brief for Petitioner at 5, Katz v. United States, 389 U.S. 347 (1967) (No. 35) (describing the recording device that captured Katz's voice as a tape recorder).

92. *See* California v. Ciraolo, 476 U.S. 207, 209 (1986) ("Officer Shutz, who was assigned to investigate, secured a private plane and flew over respondent's house at an altitude of 1,000 feet, within navigable airspace; he was accompanied by Officer Rodriguez. Both officers were trained in marijuana identification. From the overflight, the officers readily identified marijuana plants 8 feet to 10 feet in height growing in a 15- by 25-foot plot in respondent's yard . . . .").

93. *See* United States v. Knotts, 460 U.S. 276, 277 (1983) ("In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants. By monitoring the progress of a car carrying the chloroform Minnesota law enforcement agents were able to trace the can of chloroform from its place of purchase in Minneapolis, Minn[esota], to respondent's secluded cabin near Shell Lake, Wis[consin].").

94. As I have written previously, the differences in the capacity and scale of the analog technologies at issue in the Fourth Amendment canon should rightly be differentiated from new, big data surveillance capabilities. The technologies are not similar, and superficial legal analogies to old-fashioned technology does a disservice to the vitality of Fourth Amendment doctrine. *See* Ferguson, *supra* note 9, at 16 (detailing the "six A's" that differentiate analog from digital police surveillance: "(1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization").

95. For example, new policing technologies involve mass surveillance capabilities. *See* Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017).

96. *See, e.g.*, Todd Feathers, *More Cities Are Moving to Drop Automated Gunshot-Detection Tech*, VICE (Aug. 3, 2021, 8:00 AM), https://www.vice.com/en/article/88nekp/more-cities-are-moving-to-drop-automated-gunshotdetection-Tech [https://perma.cc/29W8-B7HV].

97. *See, e.g.*, Ethan McLeod, *Aerial Surveillance Planes to Begin Flying over Baltimore Friday*, BALT. BUS. J. (Apr. 30, 2020), https://www.bizjournals.com/baltimore/news/2020/04/30/aerial-surveillance-planes-to-beginflying-over.html [https://perma.cc/5PL9-VW2K].

98. *See, e.g.*, Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/locationdata-privacy-apps.html [https://perma.cc/M8CY-5SHZ].

99. *See infra* Part III.

Seeing the anti-rummaging principle as a standalone protection against government power—including police acts of information gathering—offers a new argument to limit overbroad surveillance powers.

1. Rummaging and Reasonableness

Rummaging and the fear of government agents invading private spaces, thoughts, papers, and rights—even with particularized suspicion—can be found in many Fourth Amendment opinions. As will be explored, the Supreme Court has used the term over and over to describe the unreasonableness of government overreach. These cases all share one commonality: they forbid extraneous or collateral searching of private spaces even with particularized suspicion of a crime. Because the harm of searching through sensitive material about persons, families, and things is greater than any information obtainable, the Supreme Court has drawn the line at rummaging.

a. Warrant Particularity

A clear anti-rummaging principle arises from the particularity requirement of judicial warrants.[100] The particularity language comes directly from the Fourth Amendment's requirement that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly* describing the place to be searched, and the persons or things to be seized."[101] The Supreme Court has identified the fear of rummaging as a reason why a search beyond the express particularized authorization of a warrant is unreasonable. As the Supreme Court explained in *Andresen v. Maryland*,

> "[T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory *rummaging* in a person's belongings. . . . [The Fourth Amendment addresses the problem] by requiring a 'particular description' of the things to be seized." This requirement "'makes general searches . . . impossible and prevents

100. *See* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 10 (2011) ("The Supreme Court has repeatedly explained that the Fourth Amendment's particularity requirement arose, at least in part, from the founders' concerns about British writs of assistance, general warrants issued by the king permitting soldiers to look in homes and places of business with few restrictions."); Friess, *supra* note 14, at 97 ("A central purpose served by the particularity requirement is the prevention of 'general, exploratory rummaging in a person's belongings.' The potential for such boundless rummaging is significantly magnified in the internet age, as one's private, digital conversations so infrequently remain within the periphery of one's own control." (footnote omitted) (quoting Andresen v. Maryland, 427 U.S. 463, 480 (1976))).

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

> the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"[102]

As a result, warrants must specifically authorize the search or seizure of particular goods, people, papers, etc., and cannot be the justification for exploratory searches.[103]

This anti-rummaging emphasis is explicit in the Court's reasoning in *Maryland v. Garrison*, a case involving the mistaken search of one apartment in the process of searching another.[104] In *Garrison*, even as the Court upheld the mistaken search, the Court reiterated:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.[105]

In other words, particularity tells the police what they can and cannot do, and rummaging explains the harm of why particularity is important.

In many ways, the particularity language in the Fourth Amendment is the most explicit example of the anti-rummaging principle.[106] The particularity principle means that, even with probable cause that a crime has been committed and a judicial officer's legal blessing to search a particular place, the parameters of the search cannot go beyond the particular limits in the warrant.[107] A search that extends beyond the bounds of particularity into rummaging is an unreasonable search.

---

102. *Andresen*, 427 U.S. at 480 (emphasis added) (citation omitted) (first quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); and then quoting Stanford v. Texas, 379 U.S. 476, 485 (1965)).

103. *See Coolidge*, 403 U.S. 443, 467 (1971); *see also* Commonwealth v. Freiberg, 540 N.E.2d 1289, 1300 (Mass. 1989) ("The particularity requirement serves as a safeguard against general exploratory rummaging by the police through a person's belongings."); United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999) (recognizing that the purpose of the particularity requirement is "to prevent a general exploratory rummaging in a person's belongings").

104. Maryland v. Garrison, 480 U.S. 79, 80 (1987).

105. *Id.* at 84.

106. *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 258 (2005) ("The particularity requirement prevents a 'general, exploratory rummaging in a person's belongings' and the seizure of one thing under a warrant describing another." (footnote omitted) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971))).

107. Groh v. Ramirez, 540 U.S. 551, 560 (2004) ("In this case, for example, it is at least theoretically possible that the Magistrate was satisfied that the search for weapons and explosives was justified by the showing in the affidavit, but not convinced that any evidentiary basis existed for rummaging through respondents' files and papers for receipts pertaining to the purchase or manufacture

b. Search Incident to Arrest Doctrine

Another good example of rummaging as an acknowledged harm arises in the "search incident to arrest" context.[108] The search incident to arrest doctrine allows police to search an arrestee as part of the arrest process.[109] By definition, police have probable cause to arrest the individual.[110] The rationale for the search after the arrest arises from the need to protect police officers from dangerous weapons and the need to preserve evidence that might be destroyed by the arrestee during the arrest process.[111] What the doctrine forbids, however, is using the justification of an *arrest* as a pretext to *search* for other crimes unconnected to the arrest.[112]

One rationale for this limitation on police power is a fear of rummaging. The Supreme Court has been clear that whether we are talking about homes, or cars, or digital things, the search incident to arrest doctrine does not countenance rummaging.[113] For example, in *Chimel v. California*,[114] the seminal search incident to arrest case, the Supreme Court disallowed a search of a home incident to an arrest warrant because—quoting Judge Learned Hand:

---

of such items."); *see also id.* at 561 ("We have long held, moreover, that the purpose of the particularity requirement is not limited to the prevention of general searches. A particular warrant also 'assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'" (citation omitted) (quoting United States v. Chadwick, 433 U.S. 1, 9 (1977))); Messerschmidt v. Millender, 565 U.S. 535, 558–59 (2012) (Kagan, J., concurring in part and dissenting in part) (noting that, in a qualified immunity case discussing the concern of rummaging for other evidence, "[i]n authorizing a search for all gang-related items, the warrant far outstripped the officers' probable cause").

108. *See generally* Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL'Y REV. 381, 392 (2001) (discussing the origins of the search incident to arrest doctrine).

109. *See* Seth W. Stoughton, *Modern Police Practices:* Arizona v. Gant*'s Illusory Restriction of Vehicle Searches Incident to Arrest*, 97 VA. L. REV. 1727, 1731–40 (2011) (discussing the history and evolution of the search incident to arrest doctrine).

110. A lawful arrest requires probable cause, though probable cause is not necessarily a high standard of proof. *See* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 143–84 (1st ed. 2017).

111. Knowles v. Iowa, 525 U.S. 113, 116 (1998) (recognizing "the two historical rationales for the 'search incident to arrest' exception: (1) the need to disarm the suspect in order to take him into custody, and (2) the need to preserve evidence for later use at trial" (citing United States v. Robinson, 414 U.S. 218, 234 (1973))).

112. Stoughton, *supra* note 109, at 1733 ("A search incident to arrest, held the Court, was justified under the dual rationales of officer safety and evidence gathering: it was reasonable for officers to remove any weapons with which the arrestee could 'resist arrest or effect his escape,' as well as seize any evidence to prevent its concealment or destruction. These rationales made it reasonable for officers to conduct 'a search [incident to arrest] of the arrestee's person and the area within his immediate control.' However, the Court held that there was no similar justification for searching rooms other than where the arrest was conducted, or even for searching the 'desk drawers or other closed or concealed areas in that room itself.'" (footnotes omitted) (quoting Chimel v. California, 395 U.S. 752 (1969))).

113. *See infra* notes 114, 116, 119, 121.

114. 395 U.S. 752 (1969).

> After arresting a man in his house, to *rummage* at will among his papers in search of whatever will convict him, appears to us to be indistinguishable from what might be done under a general warrant; indeed, the warrant would give more protection, for presumably it must be issued by a magistrate.[115]

Similarly, in *Arizona v. Gant*,[116] the Court made the same point about searching cars incident to arrest:

> A rule that gives police the power to conduct such a search whenever an individual is caught committing a traffic offense, when there is no basis for believing evidence of the offense might be found in the vehicle, creates a serious and recurring threat to the privacy of countless individuals. Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to *rummage at will* among a person's private effects.[117]

In a footnote, *Gant* then cites to *Boyd*, the Works of John Adams, a Ninth Circuit case, and a New Jersey case that all explicitly reference the harm of rummaging.[118] Likewise, in *Thornton v. United States*,[119] another search incident to arrest car case, Justice Scalia in the controlling concurrence criticized how the search incident to arrest doctrine had been allowed to expand:

> [I]n our search for clarity, we have now abandoned our constitutional moorings and floated to a place where the law approves of purely exploratory searches of vehicles during which officers with no definite objective or reason for the search are allowed to *rummage* around in a car to see what they might find.[120]

In other words, even with probable cause to arrest, the power to search is limited and should not include rummaging.

---

115. *Id.* at 767 (emphasis added) (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

116. 556 U.S. 332 (2009).

117. *Id.* at 345 (emphasis added).

118. *Id.* at 354 n.5 (citing Boyd v. United States, 116 U.S. 616, 624–25 (1886); JOHN ADAMS, THE WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES 247–48 (Charles Francis Adams ed., 1856); United States v. McLaughlin, 170 F.3d 889, 894 (9th Cir. 1999) (Trott, J., concurring), *abrograted by* Arizona v. Gant, 556 U.S. 332 (2009); State v. Pierce, 642 A.2d 947, 961 (N.J. 1994)).

119. 541 U.S. 615 (2004).

120. *Id.* 628–29 (Scalia, J., concurring) (emphasis added) (quoting *McLaughlin*, 170 F.3d at 894 (Trott, J., concurring)); *see also* James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417, 1472 (discussing the influence of rummaging on Justice Scalia and the search incident to arrest rationale).

As a final example, this anti-rummaging logic appeared in *Riley v. California*[121] in the digital context when police requested to examine smartphone data incident to arrest. In denying the warrantless search, the Supreme Court stated:

> In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. . . . It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. . . . The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to *rummage* at will among a person's private effects."[122]

Riley was a digital evidence case which crystalizes the harms of rummaging in the digital era. In *Riley*, the Supreme Court recognized that the storage capacity of a smartphone with all sorts of digital bits of information (photos, contacts, calendars, calls) collects too much private information in one place to not require a particularized warrant.[123] Both the quantitative and qualitative differences of the stored data risk granting too much police power to go through the digital artifacts of our lives.[124] Like the potential fear from General Warrants, the Court in *Riley* wanted to limit the ability to sift through digital clues looking for incriminating evidence incidental or outside the initial suspicion.

What is notable about the search incident to arrest cases is that the Court relied on the harm of rummaging to limit police power (even with probable cause to arrest). In other words, even though police had sufficient information to arrest a person, the Court would not allow an exploratory search beyond what was necessary for officer safety or to prevent the destruction of evidence.

c. Exceptions to the Warrant Requirement

In a series of cases involving Fourth Amendment exceptions to the warrant requirement, the Supreme Court has expressed concern about rummaging. In a variety of different situations, the Supreme Court has allowed an initial warrantless search under a recognized exception but then

121. 573 U.S. 373 (2014).

122. *Id.* at 399 (emphasis added) (quoting *Gant*, 556 U.S. at 345).

123. *See id.* at 394 ("The storage capacity of cell phones has several interrelated consequences for privacy.").

124. *See id.* at 393 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

limited that police power because of the fear of rummaging. It is the concern about rummaging that turns a constitutionally reasonable search into an unreasonable one.

For example, the "inventory exception" to the Fourth Amendment allows police to search impounded automobiles and property pursuant to an established police policy, but forbids going beyond the policy rules because "an inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence."[125] Similarly, the "plain view exception," which allows police to seize contraband discovered in a place where they have lawful access and lawful presence, cannot be expanded to search for things beyond the initial justification.[126] As the Court stated in *Texas v. Brown*:

> The Court has been sensitive to the danger inherent in such a situation [in which an officer who is executing a valid search for one item seizes a different item] that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant *to rummage* and seize at will. That danger is averted by strict attention to two of the core requirements of plain view: seizing the item must entail no significant additional invasion of privacy, and at the time of seizure the officer must have probable cause to connect the item with criminal behavior.[127]

A similar rummaging limitation exists with the "plain feel exception" based on the same type of logic.[128] A police officer may not expand their search for contraband beyond the initial justification to protect themselves against a dangerous weapon.[129] Anything beyond the initial search is considered unreasonable because it is a backdoor way to rummage for

125. Florida v. Wells, 495 U.S. 1, 4 (1990) ("Our view that standardized criteria, or established routine, must regulate the opening of containers found during inventory searches is based on the principle that an inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence. . . . The individual police officer must not be allowed so much latitude that inventory searches are turned into 'a purposeful and general means of discovering evidence of crime.'" (citations omitted) (quoting Colorado v. Bertine, 479 U.S. 367, 376 (1987) (Blackmun, J., concurring))).

126. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (recognizing that plain view searches should be as limited as possible because "the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." (emphasis removed)).

127. Texas v. Brown, 460 U.S. 730, 748–49 (1983) (Stevens, J., concurring) (emphasis added).

128. *See* Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) ("Where, as here, 'an officer who is executing a valid search for one item seizes a different item,' this Court rightly 'has been sensitive to the danger . . . that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant to rummage and seize at will.'" (quoting *Brown*, 460 U.S. at 748)).

129. *Id.*

incriminating evidence.[130] In fact, while raising very different privacy issues, the entire "reasonable suspicion"[131] doctrine can be viewed as a sort of anti-rummaging principle[132] (although one that has failed in practice).[133]

Finally, the anti-rummaging principle has been mentioned in a series of concurrences and dissents when fears of rummaging arose: for example, when the Court expanded the "hot pursuit" exception,[134] and allowed governmental employees and students to have their offices[135] and school

130. This argument has also been extended to the consent doctrine. *See* Florida v. Jardines, 569 U.S. 1, 9 (2013) ("Consent at a traffic stop to an officer's checking out an anonymous tip that there is a body in the trunk does not permit the officer to rummage through the trunk for narcotics. Here, the background social norms that invite a visitor to the front door do not invite him there to conduct a search.").

131. The "reasonable suspicion" doctrine arose as a quasi-anti-rummaging rule, cabining the ability of police to indiscriminately stop people on the streets or search people by mandating some Fourth Amendment limits. *See* L. Song Richardson, *Police Efficiency and the Fourth Amendment*, 87 IND. L.J. 1143, 1153 (2012) ("In order to protect individuals from arbitrary policing, the *Terry* doctrine requires officers to base their suspicions on specific and particular facts, not inarticulable hunches."). *Terry v. Ohio* limited the practice of unrestrained, suspicionless police stops, albeit within a legal framework that justified many such stops based on minimal suspicion. 392 U.S. 1, 12 (1968).

132. *See* Ronald S. Sullivan, Jr., *A License to Search: The Plain Feel Exception Under* Minnesota v. Dickerson*, 113 S. Ct. 2130 (1993)*, 11 HARV. BLACKLETTER L.J. 181, 189 (1994) ("*Terry* protected criminal defendants from being subjected to a police officer rummaging through their pockets and making warrantless seizures at will . . . ."); People v. Clark, 261 Cal. Rptr. 181, 183 (Cal. Ct. App. 1989) ("The reasonable suspicion requirement permits a brief perusal without allowing 'exploratory rummaging in a person's belongings.'" (quoting United States v. Weight, 667 F.2d 793, 797 (9th Cir. 1982))).

133. Lauryn P. Gouldin, *Redefining Reasonable Seizures*, 93 DENV. L. REV. 53, 70–71 (2015) ("In the nearly fifty years since *Terry*, the Court has significantly broadened the definition of reasonable suspicion and narrowed both (i) the circumstances that will be deemed a stop (instead of a mere encounter) and (ii) the circumstances that will convert a stop into an arrest (requiring probable cause). . . . The cumulative effect of these decisions—pulling back from the exigency presented in *Terry*, lengthening the time span and intrusiveness of *Terry* stops, and moving away from requiring specificity about the offense of suspicion—is readily seen in the dramatic increase in the use of stops and frisks as a regulatory or deterrent tool to manage crime in urban communities." (footnote omitted)). Investigations and lawsuits in New York City, Chicago, and Baltimore, among other large cities, have showed systemic stop and frisk violations based on the reasonable suspicion standard. Floyd v. City of New York, 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) ("The City acted with deliberate indifference toward the NYPD's practice of making unconstitutional stops and conducting unconstitutional frisks."); U.S. DEP'T OF JUST.: C.R. DIV. & U.S. ATT'YS OFF. N. DIST. OF ILL., INVESTIGATION OF THE CHICAGO POLICE DEPARTMENT 102 (2017), https://www.justice.gov/opa/file/925846/download [https://perma.cc/U8W6-6C9G]; U.S. DEP'T OF JUST.: C.R. DIV., INVESTIGATION OF THE BALTIMORE CITY POLICE DEPARTMENT 24 (2016), https://www.justice.gov/crt/file/883296/download [https://perma.cc/U4CT-49ZN].

134. *See* Warden v. Hayden, 387 U.S. 294, 311 (1967) (Fortas, J., concurring) ("[W]e have forbidden the use of articles seized in such a search unless obtained from the person of the suspect or from the immediate vicinity. Since a warrantless search is justified only as incident to an arrest or 'hot pursuit,' this Court and others have held that its scope does not include permission to search the entire building in which the arrests occurs, or to rummage through locked drawers and closets, or to search at another time or place.").

135. *See* O'Connor v. Ortega, 480 U.S. 709, 736 (1987) (Blackmun, J., dissenting) (government employee search) ("Moreover, as the plurality itself recognizes, the 'investigators' never made a formal inventory of what they found in Dr. Ortega's office. Rather, they rummaged through his belongings and seized highly personal items later used at a termination proceeding to impeach a witness favorable to him." (citation omitted)).

lockers[136] searched on less than probable cause. While not carrying the day, the arguments about the harm of rummaging were explicit in the Justices' opinions and show that rummaging harms remain a key part of analyzing Fourth Amendment reasonableness.

d. Conclusion on Rummaging and Reasonableness

These Fourth Amendment reasonableness cases share several commonalities in regards to rummaging. First, they recognize rummaging as a limitation on police power. The initial justification (or exception) controls the scope of what further information police can obtain. Second, the rummaging principle provides a form of practical notice to police about those *ex ante* limits. It is known beforehand that such additional investigation is forbidden. Third, and most importantly, the principle stops the rummaging from happening, limiting the privacy and liberty harms. Even with individualized suspicion of particular criminal activities, the rummaging principle pushes back against the additional collection of information outside those particular circumstances. Rummaging as a rule of reasonableness, thus, is well supported in the doctrine.

In contrast, when the Supreme Court has focused on the threshold search question[137]—i.e., whether the Fourth Amendment even applies—rummaging has been largely ignored. As will be explained in the next Section, this was partially a quirk of history—namely, at the time the "reasonable expectation of privacy" test was created, existing police surveillance technology did not allow the technical ability to rummage. This next Section will explain why this history must be reexamined in the digital age with greater rummaging capabilities at issue.

2. Rummaging and Reasonable Expectations of Privacy

The analysis of *rummaging and reasonableness* largely focused on what police could do with both a lawful justification and particularized suspicion. The question of *rummaging and reasonable expectations of privacy* focuses a bit earlier in the investigatory process. The Supreme Court has framed the question as a threshold test of whether the Fourth Amendment even applies to government action. Under current doctrine, one way to answer the

136. *See* New Jersey v. T.L.O., 469 U.S. 325, 381–82 (1985) (Stevens, J., concurring) (student search) ("Moreover, the majority's application of its standard in this case—to permit a male administrator to rummage through the purse of a female high school student in order to obtain evidence that she was smoking in a bathroom—raises grave doubts in my mind whether its effort will be effective. Unlike the Court, I believe the nature of the suspected infraction is a matter of first importance in deciding whether *any* invasion of privacy is permissible." (footnote omitted)).

137. *See supra* note 11 and accompanying text (discussing the role of the threshold search question in Fourth Amendment doctrine).

question of whether the Fourth Amendment applies (i.e., whether a search has occurred) is for courts to ask whether an individual's "reasonable expectation of privacy" has been violated.[138] If so, then the court is required to address whether the governmental action required a warrant or whether an exception applies. If there is no violation of a reasonable expectation of privacy, then there is no Fourth Amendment search (and no constitutional bar to the police action).

Many scholars and judges have acknowledged that the reasonable expectation of privacy test is incoherent and ad hoc.[139] Some Justices have even advocated for abandoning the test altogether.[140] Worse, the rule—admittedly confusing enough in a physical, analog world where people could at least intuitively understand the limits of human surveillance—becomes completely unmoored in a digital age with technologies providing superhuman surveillance powers that can literally see, hear, and sense things in new ways.[141]

While it would be overstating things to say that the rummaging principle can resolve the current doctrinal muddle, identifying the rummaging harms does offer a new insight to the constitutional analysis. This Section begins by looking at why the Supreme Court largely ignored rummaging in early reasonable expectation of privacy cases, and then examines why it has been reincorporated into its recent digital policing cases.

a. Analog Surveillance Technologies

At the outset, it is important to note that for much of the late twentieth century (when the reasonable expectation of privacy doctrine was being

138. Justice Scalia in *Jones* also reclaimed the trespass test as part of the Fourth Amendment threshold calculus. *See* United States v. Jones, 565 U.S. 400, 409 (2012).

139. *See, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence.").

140. *See* Carpenter v. United States, 585 U.S. 296, 343 (2018) (Thomas, J., dissenting) ("The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence."); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable.").

141. *See* Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the* Carpenter *Decision*, 16 OHIO ST. J. CRIM. L. 281, 287 (2018) (discussing police technologies that are "superhuman, passive, and automated"); Kate Weisburd, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 N.C. L. REV. 717, 721 (2020) ("The Court has likewise recognized that the concept of a 'reasonable expectation of privacy' for Fourth Amendment purposes must reflect the 'seismic shifts in digital technology' that now allow for 'near perfect surveillance' of digital records that 'hold for many Americans the "privacies of life."' These efforts reflect a bipartisan consensus that, when it comes to government surveillance of private citizens, 'digital is different.'" (footnotes omitted) (first quoting *Carpenter*, 585 U.S. at 313; then quoting *id.* at 297; and then quoting Riley v. California, 573 U.S. 373, 403 (2014))).

developed), the surveillance technologies at issue were relatively simple tools.[142] *Katz v. United States* involved an audio recording device (essentially a large cassette tape player) physically affixed to the top of a stand-alone, coin-operated phone booth.[143] *Knotts v. United States* involved a beeper that required physically proximate human officers to track the radio frequencies.[144] *Kyllo v. United States* involved a thermal imaging device that merely recorded external heat levels emanating off a house.[145] One reason why rummaging was not front and center in the early expectation of privacy debates is that the analog technologies at issue did not allow for significant extraneous or ancillary data collection. In other words, the technology was so rudimentary that it could not conduct generalized surveillance for long periods of time or against numerous people.

This is not to say that rummaging did not emerge as a background concern in thinking about the scope of reasonable expectations of privacy. A good example is to compare the *Katz* case with the underlying debates about eavesdropping/wiretapping. As is familiar to most criminal procedure students, *Katz v. United States* involved the recording of several incriminating phone calls used to demonstrate that Charlie Katz was involved in an illegal gambling operation.[146] Katz moved to suppress the evidence by arguing that the warrantless collection of his conversations was a search for Fourth Amendment purposes.[147] The Supreme Court held that the police collection was a search because Katz had tried to maintain the privacy of the call, and in a now controlling concurring opinion, Justice Harlan detailed what we now know as the reasonable expectation of privacy test.[148]

What is less well known is that *Katz* was decided in the shadow of the Supreme Court's eavesdropping/wiretapping debate—a debate that centered on the overbroad attempt to secretly record and rummage through personal conversations for long periods of time.[149] In 1967, the same year

142. *See* Ferguson, *supra* note 4, at 824.

143. Brief for Petitioner at 5, Katz v. United States, 389 U.S. 347 (1967) (No. 35) ("Petitioner's conversation was overheard and recorded [and later transcribed] by means of a tape recorder which was placed on top of the middle booth. One of the three booths was placed out of order by the FBI with the consent of the telephone company." (citation omitted)).

144. *See* David H. Goetz, *Locating Location Privacy*, 26 BERKELEY TECH. L.J. 823, 839 (2011) ("[T]he beepers used in *Knotts* and *Karo* were simple radio transmitters of limited range that forced the agents tracking the device to stay in close physical proximity to the device." (footnote omitted)).

145. *See* Brief for Respondent at 7, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508) ("When a thermal imager is pointed at a wall composed of normal construction materials, such as lath, plaster, plasterboard, stucco, or brick, it detects the radiation that is emitted or reflected from the outside surface of the wall. An imager cannot see through a wall.").

146. *Katz*, 389 U.S. at 348.

147. *Id.*

148. *Id.* at 360–61 (Harlan, J., concurring).

149. *See* Berger v. New York, 388 U.S. 41, 44 (1967).

as *Katz*, the Supreme Court decided *Berger v. New York*, a case involving a Fourth Amendment challenge to a New York State eavesdropping law that allowed police to bug offices and record conversations for months at a time.[150] In striking down the eavesdropping statute, the Supreme Court explicitly called out the dangers of overbroad and indiscriminate collection of personal, private information, liking it to a General Warrant.[151] In finding the New York eavesdropping statute violated the Fourth Amendment, the Court emphasized that listening to conversations without time limits, or cabined to particularized substantive subject areas, just left too much discretion in the hands of the officers to randomly listen to everything.[152] Even if criminal conversations might be uncovered, the privacy intrusions were too grave to countenance that method of overbroad evidence collection. The explicit fear was that police officers could rummage through the conversations of suspects and find incriminating facts among the many other personal communications just like the agents investigating Wilkes or Entick.[153] In a concurring opinion, Justice Douglas went even further and stated that such conversations should never be recorded (even with a specific warrant).[154] The harm again was that information once-removed from the initial suspicion could be used by the government to prosecute disfavored individuals.[155]

150. *Id.* at 44–45.

151. *Id.* at 58 (describing the history of the Fourth Amendment and General Warrants and stating that the New York eavesdropping statute was "equally offensive").

152. *Id.* at 59.

153. *See, e.g.*, United States v. U.S. Dist. Ct., 407 U.S. 297, 325 (1972) ("Here, federal agents wish to rummage for months on end through every conversation, no matter how intimate or personal, carried over selected telephone lines, simply to seize those few utterances which may add to their sense of the pulse of a domestic underground. We are told that one national security wiretap lasted for 14 months and monitored over 900 conversations.").

154. *Berger*, 388 U.S. at 67 (Douglas, J., concurring) ("The history of the Fourth Amendment . . . makes it plain that any search in the precincts of the home for personal items that are lawfully possessed and not articles of a crime is 'unreasonable.' That is the essence of the 'mere evidence' rule that long obtained until overruled by *Hayden*.").

155. Of course, the debate over wiretaps, rummaging, and the Fourth Amendment go back to *Olmstead v. United States*, 277 U.S. 438 (1928), *overuled by* Katz v. United States, 389 U.S. 347 (1967). The majority in *Olmstead* found no Fourth Amendment violation, *id.* at 466, but Justice Brandeis in a famous dissent set the stage for a privacy-focused Fourth Amendment. *Id.* at 475–76 (Brandeis, J., dissenting). Brandeis was joined in this view by Justice Butler. *See* Russell L. Weaver, *The Fourth Amendment: History, Purpose, and Remedies*, 52 TEX. TECH L. REV. 127, 132 (2019) ("Justice Butler also dissented in *Olmstead* and argued for a more expansive interpretation of the Fourth Amendment. Since 'communications belong to the parties between whom they pass,' and 'the exclusive use of the wire belongs to the persons served by it,' he viewed wiretapping as a search within the meaning of the Fourth Amendment. He argued that 'the Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words,' and he viewed the monitoring of phone lines as equivalent to colonial officials rummaging through a house." (footnotes omitted) (quoting *Olmstead*, 277 U.S. at 485–88 (Butler, J., dissenting))).

With this background, the argument in *Katz*, which did not directly address rummaging, was, in fact, shaped by the rummaging debate.[156] One might imagine if the collection of conversations in *Katz* was longer, broader, or covered more people, the same arguments seen in *Berger* would have been raised and rummaging directly addressed.[157] And, notably, the Title III Wiretap Act legislation enacted in response to *Katz* did include anti-rummaging principles such as minimization requirements, particularity standards, a probable cause plus standard, and other legal protections.[158] Thus, while rummaging did not take center stage in the creation of the reasonable expectation of privacy doctrine, it did have a supporting role.

That said, rummaging fears did not directly arise in the early post-*Katz* cases. In the 1970–1990's, the reasonable expectation of privacy doctrine—birthed in *Katz*—was interpreted permissively to allow expanded police surveillance. The Supreme Court allowed beepers to track cars,[159] planes to fly over homes and view suspected marijuana plants,[160] and phone numbers and bank records to be turned over to investigators[161] all without violating a reasonable expectation of privacy or requiring a warrant. These cases involved relatively discrete surveillance activities with simplistic technologies and with little to no debate about rummaging harms. The point here is not that these cases were wrongly decided (although perhaps some were) but that the lack of focus on rummaging can be explained by the fact that the technology at issue could not really rummage for much extraneous information.[162]

156. *See* United States v. Jones, 565 U.S. 400, 427–28 (2012) ("On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U.S.C. §§ 2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.").

157. *Katz*, of course, was not a case of lengthy overcollection but instead a targeted investigation of a specific person with specific calls.

158. *See* 18 U.S.C. § 2518.

159. United States v. Knotts, 460 U.S. 276, 282 (1983).

160. California v. Ciraolo, 476 U.S. 207, 209 (1986); Florida. v. Riley, 488 U.S. 445, 448 (1989).

161. Smith v. Maryland, 442 U.S. 735, 737 (1979); United States v. Miller, 425 U.S. 435, 437–38 (1976).

162. For example, in *United States v. Knotts*, the Supreme Court held that police use of a beeper to track a suspect on public roads was not a search because movements in public deserve no expectation of privacy. 460 U.S. at 281 ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). Viewed in isolation, there might not be much concern about rummaging from a single beeper and a single suspect's travels. The analysis, however, might be looked at differently if the rummaging principle were considered, since the Court's holding implicitly allows warrantless tracking for any or no reason against everyone, anywhere in public. It is for this reason that the Court felt it necessary to clarify its holding by warning about more extensive surveillance techniques:

One can go through the traditional Fourth Amendment canon looking at how the Court cabined its analysis to avoid addressing the rummaging issue and come up with similar results.[163] If there is no expectation of privacy for phone numbers captured by a pen register as in *Maryland v. Smith*, then there is nothing stopping police from using a pen register to rummage through all phone numbers from all people for any reason.[164] If there is no expectation of privacy for bank records for one person as in *Miller v. United States*, then there is nothing stopping police from rummaging through all bank records of all persons.[165] In focusing on expectations of privacy, and not the act of going through everyone's information, the outcome is different. One could imagine broader collections of more phone numbers or bank records might result in a different privacy analysis if viewed through

> Respondent . . . expresses the generalized view that the result of the holding sought by the government would be that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." . . . [I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.

Id. at 283–84 (quoting Brief for Respondent at 9, United States v. Knotts, 460 U.S. 276 (1983) (No. 81-1802)). Or, in other words, if the Court were forced to consider the harm of rummaging using more generalized surveillance, it might need to come out with a different Fourth Amendment result. This understanding was confirmed in *Carpenter*. *See Carpenter v. United States*, 585 U.S. 296, 306–07 (2018) ("This Court in *Knotts,* however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. The Court emphasized the 'limited use which the government made of the signals from this particular beeper' during a discrete 'automotive journey.' Significantly, the Court reserved the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country [were] possible.'" (citation omitted) (quoting *Knotts*, 460 U.S. at 1081)).

163. For example, *California v. Ciraolo*, 476 U.S. at 209, and *Florida v. Riley*, 488 U.S. at 448, both involved police investigators flying over private backyards in a plane or helicopter to observe illegal marijuana plants. The constitutional question was whether these human observations were "searches" for Fourth Amendment purposes, and the test again asked whether the observations violated a reasonable expectation of privacy. *Ciraolo*, 476 U.S. at 213–14 (finding no expectation of privacy from a plane in public airspace); *Riley*, 488 U.S. at 450 ("The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye." (quoting *Ciraolo*, 476 U.S. at 215)). The Supreme Court held that neither police action was a Fourth Amendment search because the human observations did not violate a reasonable expectation of privacy.

Viewed in isolation, a single flight over a single backyard raises little fear of rummaging. Of course, if rummaging is added to the analysis things might change. The reality is that investigative flights involve multiple observations of many properties. Just because the investigators chose to focus their eyes on Ciraolo's or Riley's property does not mean the Fourth Amendment required this limit. Under the Court's reasoning, any sighting of any property from the same vantage point would have been constitutionally permissible. Police officers at any time could fly over any house as many times as they like, and if anything was spotted, there would be no Fourth Amendment search claim as long as police were in lawful airspace. In narrowing the discussion to the one observation, the Court ignored the rummaging harms of being able to do this type of overbroad surveillance whenever and for whatever reason. The dissents raised this very point, citing to *Boyd*, the harm of rummaging, and the privacy values of the Fourth Amendment. *See Ciraolo*, 476 U.S. at 217, 226 (Powell, J., dissenting); *Riley*, 488 U.S. at 461–62 (Brennan, J., dissenting).

164. *See Smith*, 442 U.S. at 741.

165. *See Miller*, 425 U.S. at 442–43.

a rummaging frame. In fact, while beyond the scope of this Article, one could reinterpret the entire Fourth Amendment canon through the rummaging principle and reach different results. And, as will be discussed in the next Section, that is precisely what has happened in more modern digital surveillance cases.

b. Digital Is Different

Over time, as police shifted from the analog surveillance technologies of the twentieth century to the digital investigative systems of the twenty-first century, the Supreme Court had to reassess its approach to the threshold search question. Notably in two cases—*Carpenter v. United States*[166] and *United States v. Jones*[167]—the Court recognized that the scale and scope of digital surveillance necessitated a new approach to the reasonable expectation of privacy analysis.[168] This Section seeks to explore how the harm of rummaging has shaped this new understanding.

Much scholarly ink has already been spilled explaining how the Supreme Court's "digital is different" cases change the reasonable expectation of privacy analysis.[169] This Article seeks to do something different by looking at the Supreme Court's decision through the lens of rummaging. My argument is that the rummaging principle, and not the traditional reasonable expectation of privacy rationale, offers a better way to understand the harm of new surveillance threats.

Carpenter v. United States offers a clear example.[170] As mentioned, this case turned on a law enforcement subpoena for cell site location information (CSLI) from two private phone companies.[171] The government suspected that Timothy Carpenter was involved in a series of robberies and sought the cell phone location data to bolster their case that he was at the robbed stores. Police used a court order (not a warrant) to obtain the location data, and because of the way cell phone data works, the records offered a rough

166. 585 U.S. 296 (2018).

167. 565 U.S. 400 (2012).

168. Scholars have recognized that *Riley*, *Jones*, and *Carpenter* signify a "digital is different" framework for Fourth Amendment analysis. *See, e.g.*, Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 951 (2016).

169. *See* Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 216 (2018) ("*Carpenter* is the latest in a trilogy of decisions in which the Supreme Court has finally begun to confront modern surveillance tools used by law enforcement."); *see also* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1794 (2022); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 369 (2019).

170. 585 U.S. 296 (2018).

171. *See* Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 497 (2017) (describing the facts of the case).

approximation of Carpenter's daily movements.[172] The requested data included thousands of pages of data detailing his location over time. Carpenter objected on Fourth Amendment grounds, arguing that acquiring this data violated a reasonable expectation of privacy and required a probable cause warrant.[173]

Unlike the analog surveillance cases, the Supreme Court did not focus on Mr. Carpenter's presence in a public space, his reliance on private third-party cell phone providers, or even the relatively unilluminating location information at the time of the robberies. After all, Carpenter was travelling in public, using a third-party service, and the only personal facts revealed were a few moments he was present in some electronic stores (participating in a robbery). Instead, the Supreme Court focused on the potential revealing nature of the cell networks at issue and the danger presented in giving police unlimited ability to rummage through the data to find incriminating clues.[174] As the Court stated, "[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[175] Or rephrased, the case was about the government's ability to rummage through that detailed chronicle of digital trails.

In *Carpenter*, the Supreme Court centered the harm of digital rummaging (without necessarily naming it as such). Critical to Chief Justice Robert's argument are three points. First, that government access to locational data could reveal private information beyond (or incidental to) any involvement in criminal activities.[176] Instead of simply focusing on the actual locations revealed (a few electronics stores), the Court focused on the potential police power to identify movements and locations with personal meaning incidental to any criminal activity:

> Allowing government access to cell-site records contravenes that expectation [of privacy]. . . . Mapping a cell phone's location over

172. *Carpenter*, 585 U.S. at 301 ("[T]he prosecutors applied for court orders under the Stored Communications Act . . . .); *see also id.* at 302 ("The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was 'roaming' in northeastern Ohio.").

173. *Id.* ("Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause."); *see also id.* at 310–13.

174. *Id.* at 311 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring))).

175. *Id.* at 315.

176. *Id.* at 312.

> the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." These location records "hold for many Americans the 'privacies of life.'"[177]

This shift in focus is important because it moves the Court away from the narrow question of the crime at issue to the broader fear of what could be discovered incidental to or independent of the crime by government snooping. Akin to the fears of finding incriminating materials among the search for seditious papers, the Court appears as much concerned with what could be found by rummaging through the locational data as it was with the information actually found.

Second, the Court emphasized that the cell site technology provides a power to retroactively rummage for wrongdoing (beyond a specific suspected crime).[178] The stored dataset of locational clues allowed police the ability to find any past activity.[179] Unlike the audio recording device, beepers, thermal imagers, and pen registers of the analog world, this digital technology now allows retrospective searches of vast stores of collected information. It is not just searching adjacent to suspicious things but also the ability to search historically for suspicious activities not yet discovered. If no warrant is required, such inquiries could be undertaken without suspicion or any justification, allowing police to rummage for past wrongdoing (again independent of the suspected crime). As the Court in *Carpenter* acknowledged:

> [T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices [sic] of the wireless carriers, which currently maintain records for up to five years.[180]

Third, the Court emphasized that warrantless access to such a database of location information would allow searches against anyone, not just those for whom there is suspicion.[181] The potential for mass queries and overbroad

177. *Id.* at 311 (first quoting quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); and then quoting Riley v. California, 573 U.S. 373, 403 (2014)).

178. *Id.* at 312.

179. *Id.*

180. *Id.*

181. *Id.*

investigations (against the innocent and guilty alike) concerned the Court enough to write:

> Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. . . . Only the few without cell phones could escape this tireless and absolute surveillance.[182]

Each of these points show the harms of rummaging through data in overbroad and unlimited ways. These concerns led the Court to find that the acquiring of seven days of cell site data violated a reasonable expectation of privacy.[183] And, importantly for digital rummaging purposes, the case supports that such rummaging runs counter to Fourth Amendment history,[184] the Founders' concern with arbitrary searches,[185] and fear of permeating police surveillance.[186]

The *Carpenter* Court drew support for its holding from the concurring opinions in *United States v. Jones*[187] and the search incident to arrest case of *Riley v. California*[188]—both digital is different cases. *Jones* involved the long-term (twenty-eight-day) warrantless tracking of a suspected drug dealer.[189] Antoine Jones moved to suppress the tracking information obtained via GPS that linked him to a suspected stash house of illegal narcotics.[190] The majority of the Court held that placing the GPS tracker on the vehicle was a physical intrusion into a constitutionally protected area and thus a trespass search for Fourth Amendment purposes.[191] But more importantly for purposes here, five Justices concurred in the judgment,

182. *Id.*

183. *Id.* at 313 ("[W]hen the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.").

184. *See id.* at 304–05 ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.'" (footnote omitted) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925))).

185. *Id.* at 305 ("On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

186. *Id.* ("Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

187. 565 U.S. 400 (2012).

188. 573 U.S. 373, 386 (2014).

189. *Jones*, 565 U.S. at 403.

190. *Id.*

191. *Id.* at 404–05 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

reasoning that long-term tracking for most crimes violated a reasonable expectation of privacy.[192] The concurring Justices' view that long-term locational tracking violated a reasonable expectation of privacy was explicitly acknowledged in *Carpenter*.[193]

For purposes of examining rummaging, *Jones* is helpful because, like *Carpenter*, it identifies the harms of granting unlimited government surveillance powers.[194] Again, it is important to note that the concurring Justices did not just focus on the specific tracking data that linked Jones to the drug stash house but instead focused on the general location data that potentially could have been uncovered about his personal life and interests. It was not what was actually discovered about Jones but the harm of what could be discovered if investigating officers had access to rummage through the clues of his life.

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The government can store such records and efficiently mine them for information years into the future.[195]

This is the harm of rummaging linked to a reasonable expectation of privacy in the digital context. Both Justice Sotomayor and Justice Alito—in their two separate concurring opinions in *Jones*—reiterated the harm of how digital technologies will grant police dangerous rummaging powers.[196] Justice Sotomayor discussed the chilling nature of potential surveillance that undermines expressive freedom and reveals private identity formation habits.[197] Justice Alito detailed the harms of creating a catalogue of daily movements that undermined expectations to travel without being monitored.[198] Both Justices foreshadowed how the Court in *Carpenter*

192. *See id.* at 413–16 (Sotomayor, J., concurring); *id.* at 429–31 (Alito, J., concurring in judgment).

193. As Chief Justice Roberts wrote in *Carpenter*, "A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." Carpenter v. United States, 585 U.S. 296, 310 (2018) (citing *Jones*, 565 U.S. at 430).

194. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

195. *Id.* at 415 (citation omitted).

196. *Id.* at 413–16; *id.* at 429–31 (Alito, J., concurring).

197. *See id.* at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring))).

198. *See id.* (Alito, J., concurring in judgment) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's

would see the harms of long-term location tracking as an arbitrary and overbroad police power.

c. Conclusion on Rummaging and Reasonable Expectations of Privacy

Rummaging has not always been a good fit for the reasonable expectation of privacy doctrine. The early cases about reasonable expectations of privacy turned on technologies that did not raise rummaging fears. Simple, human-centered technologies of surveillance just did not raise the same concerns as larger-scale digital surveillance systems.

As this changed, the Supreme Court borrowed the logic of rummaging to address the digital search harms. The Court harkened back to the principles of *Entick* and *Boyd* and tried to articulate a reason why broad potential search powers violate the Fourth Amendment.[199] While not stating it as directly as this Article seeks to do, the upshot of the Supreme Court's reliance on rummaging harms is clear. The next Part will attempt to turn this insight about rummaging into an operational principle for future analysis.

II. THE RUMMAGING PRINCIPLE

The first Part of this Article demonstrated how rummaging has influenced Fourth Amendment theory and outcomes. This second Part will demonstrate how the rummaging principle can be turned into a standalone Fourth Amendment framework. Specifically, this Part distills the rummaging analysis discussed in Part I into a workable test that can be applied to new digital challenges like smart homes or digital pole camera systems (which will be discussed in Part III). In simple terms, any police action that fails the rummaging test will be deemed a violation of the Fourth Amendment.

To build out this test, it is important to identify why rummaging has mattered as a Fourth Amendment concern. Rummaging is an act, but it is more than a physical act that raises Fourth Amendment problems. It is the grant of power or technological ability to rummage that also threatens Fourth Amendment security.

More plainly, while agents acting under the authority of the Writs of Assistance or General Warrants clearly violate rummaging principles, even if the agents never acted, the grant of authority—the power—to rummage would still create constitutional harm. Thus, it is important to identify what

expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

199. *See supra* notes 184–86 and accompanying text.

are the core privacy and security harms that gave rise to the Fourth Amendment. Once the harms are identified, then the guidelines of what constitutes unreasonable rummaging can be defined into a framework/test.

This first Section seeks to explain rummaging harms by synthesizing the various concerns that kept reappearing in the cases discussed in Part I.

A. Rummaging Harms

The overall goal of this Article is to show that police rummaging is a cognizable Fourth Amendment harm relevant for both determining that there has been a search and for the ultimate question of reasonableness. As I will argue, rummaging as a grant of legal or technological power to intrude on personal spaces, activities, papers, and thoughts without particularized limitations should be considered an unreasonable search and thus a violation of the Fourth Amendment. Rummaging harms can manifest as a legislative enactment—like a modern-day Writs of Assistance—or in police use of a surveillance technology—like long-term CSLI tracking—both of which allow for unbounded police surveillance power.

Building off the history and cases discussed in Part I, this Section synthesizes the various harms of rummaging discussed earlier. This Section explores four interrelated harms arising from the power to rummage, specifically, (1) arbitrary enforcement of police power ("arbitrariness"); (2) overreaching exploratory expansions of initially justified searches ("overreach"); (3) intrusions into constitutionally protected interests (e.g., homes, persons, papers, effects) ("intrusion"); and (4) exposure of private details as a form of political or social control ("exposure"). As will become evident, while arising from a physical, analog, and sometimes quite old-fashioned world, the rummaging principle neatly fits the digital age.[200]

1. Arbitrariness

The first harm that can be divined from the cases discussed in Part I involves the harm of arbitrary policing. Rummaging raises concern about arbitrary police power. One way to see the Fourth Amendment is to view it as a restriction on unlimited governmental enforcement power.[201]

---

200. *See* Gerald S. Reamey, *Constitutional Shapeshifting: Giving the Fourth Amendment Substance in the Technology Driven World of Criminal Investigation*, 14 STAN. J. C.R. & C.L. 201, 221 (2018) ("If the principal evil against which the Fourth Amendment was aimed was the entry into one's home and rummaging through one's effects, prohibiting a 'virtual' entry and rummaging by technological means in the Twenty-First Century seems consistent with the values of the Framers.").

201. Carpenter v. United States, 585 U.S. 296, 305 (2018) ("[O]ur cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a

The harm of arbitrary police power has long animated Fourth Amendment cases.[202] Examples include abusive treatment toward individuals, including cases which involve unreasonable interference with individual liberty or property.[203] Whether we are talking about street stops,[204] car stops,[205] or unwarranted searches of homes,[206] the examples of police searches and seizures in an arbitrary manner is reflected in decades of cases.

In addition, arbitrary enforcement creates collective harms running to entire communities.[207] After all, rummaging under the power of General Warrants or Writs of Assistance marked the entire community as a target.[208] As Professor David Gray has recognized, the Fourth Amendment can be conceived of as a collective right, expressing a community assertion of

---

too permeating police surveillance.'" (citation omitted) (first quoting quoting Boyd v. United States, 116 U.S. 616, 630 (1886); and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

202. *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 242 (1973) ("[T]he Fourth Amendment protects the 'security of one's privacy against arbitrary intrusion by the police.'" (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949))); *see also* Alan C. Michaels, *Rights Knowledge: Values and Tradeoffs*, 39 TEX. TECH L. REV. 1355, 1373 (2007) ("A third purpose conceived for the right against unreasonable searches is to guard against arbitrary or discriminatory use of the police power. That is, to prevent the police from using 'discretion to target [an individual] for unfavorable treatment without a legitimate basis.'" (quoting Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1472 (1996))); FRIEDMAN, *supra* note 110, at 143–84.

203. *See, e.g.*, Delaware v. Prouse, 440 U.S. 648, 653–54 (1979) ("The essential purpose of the proscriptions in the Fourth Amendment is to impose a standard of 'reasonableness' upon the exercise of discretion by government officials, including law enforcement agents, in order 'to safeguard the privacy and security of individuals against arbitrary invasions . . . .'" (footnote omitted) (quoting Marshall v. Barlow's, Inc., 436 U.S. 307, 312 (1978))); United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976) ("The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.").

204. *See* Louis Michael Seidman, *The Problems with Privacy's Problem*, 93 MICH. L. REV. 1079, 1089 (1995) ("Consider searches on the street, for example. We must not lose sight of the fact that these searches also amount to a species of violence. A typical search requires the police to delay a suspect who is going about his business, force him to assume a vulnerable and uncomfortable position, embarrass him before others, and touch all parts of his body.").

205. *See* United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975) ("As with other categories of police action subject to Fourth Amendment constraints, the reasonableness of such seizures depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers.").

206. *See* Thomas P. Crocker, *The Fourth Amendment at Home*, 96 IND. L.J. 167, 168 (2020) ("Fourth Amendment text places special emphasis on securing protections for the home—in addition to persons, papers, and effects—against unwarranted government intrusion.").

207. *See* David Gray, *Collective Rights and the Fourth Amendment After* Carpenter, 79 MD. L. REV. 66, 82 (2019) ("The collective nature of the Fourth Amendment is even more evident when we consider the precise nature of the right it enshrines. The Fourth Amendment does not prohibit searches and seizures. It does not even prohibit unreasonable searches and seizures. Instead, it guarantees a right 'to be secure' against unreasonable searches and seizures. It commands that 'the people' shall live in a state free from fear of being the targets of unreasonable searches and seizures—and particularly searches and seizures wielded as tools to punish disfavored political and religious groups.").

208. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 679 n.363 (1999) ("[T]he collective tone of 'the people' is appropriate to a provision banning *general* warrants because such warrants, if allowed, would imperil the security of the entire community.").

liberty against government surveillance.[209] Rummaging weakens that collective security from government enforcement actions.

It is no accident then that the anti-arbitrariness concept regularly appears in Fourth Amendment cases and makes a central appearance in digital surveillance cases.[210] The limitless nature of police discretion, the lack of oversight, the lack of notice, and the contingent nature of police enforcement threats speak to an imbalance of power, a concern of political intimidation, and the chilling effects of broadly sweeping police enforcement.[211] Without a constitutional check, the potential to abuse the enforcement power is too great.

2. Overreach

Rummaging also reflects a concern about overreaching government power. Overreach involves the related harm of having police uncover incriminating information incidental to or outside of the original justification for an inquiry. As has been discussed, the reasonableness cases detailed in Section I.B.1 demonstrate the concern of using one justified intrusion as grounds for exploratory investigations to seek additional incriminating facts.[212]

---

209. David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189, 191 (2015).

210. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 462 (1989) (Brennan, J., dissenting) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." (quoting Marshall v. Barlow's, Inc., 436 U.S. 307, 312 (1978))); INS v. Delgado, 466 U.S. 210, 215 (1984) ("The Fourth Amendment does not proscribe all contact between the police and citizens, but is designed 'to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.'" (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976))).

211. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 95 (2013) ("Although the negative rights afforded by the Fourth Amendment have specific historical antecedents, the text itself evinces a broader historical purpose to protect against indiscriminate and invasive governmental practices that are characteristic of a surveillance state."); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 31 (2013) ("[A] dragnet that catches thousands of travelers or other citizens is not the only kind of sweeping investigatory technique that offends Fourth Amendment purposes. For example, dragnet investigations under which officers rummage through possessions or drawers of documents without justification also offend these purposes, even when the hunt for unknown contraband occurs within a single home and focuses on the property of a single homeowner. A government 'fishing expedition' should likewise be deemed to be subject to Fourth Amendment constraints when the data that officials sift through comes not from personal documents, but from the trail of data people leave behind in a world in which every action or movement is recorded for potential review at a later date." (footnote omitted)).

212. *See supra* Section I.B.1; *see also* Sacharoff, *supra* note 34, at 1653 ("[R]ummaging through papers for new crimes is the very definition, for both the founding generation and contemporary courts, of the fishing expedition the Fourth Amendment (and likely Fifth Amendment) sought to prevent." (footnotes omitted)).

First, as to intentional overreach, the fear is that, by rummaging, police will find incriminating information once removed from the original justification for the search. Essentially, the overreach concern is that police will be able to use the probable cause pretext about one crime to search for other crimes for which they do not have probable cause.[213] This purposeful extension of initially justified suspicion is the type of search frowned on by the Founders.[214]

As a related concern, rummaging is necessarily overinclusive, even when there is no intentional overreach.[215] The search process likely captures innocent conduct and innocent people.[216] Rummaging can uncover evidence about other people not connected to the initial justification. Sometimes those people are caught doing a criminal act, but many times their actions are completely innocent and yet their lives and privacy are revealed by police investigation.[217]

The digital nature of evidence makes these overreach concerns even more problematic. Because things are digital, the data can be saved and searched later in time. The harms are not just what happens during the search but the continuing harms arising from having large datasets of collected information that can be queried at any time.[218] The power to

213. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467–69 (1971) (discussing the limits of the plain view doctrine, which prohibits searching beyond the justification of the search warrant unless the item in question is immediately recognizable as evidence).

214. *See* Donohue, *supra* note 40, at 1284 ("Concerns about general warrants, and about ensuring that specific warrants contained sufficient particularity, figured largely in the conversation, which centered on ensuring that the rights of the people would be secure against government overreach.").

215. *See* Cassady v. Goering, 567 F.3d 628, 643 (10th Cir. 2009) ("The purpose of the Fourth Amendment extends beyond merely preventing intentional abuses of warrant procedure, however. As the Supreme Court said in *Coolidge*, '[T]he specific evil is the "general warrant" abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings.'" (citation omitted) (quoting *Coolidge*, 403 U.S. at 467)).

216. *See* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 57 (2018) ("[A]ny digital storage medium seized because it contains evidence of criminality will also include vast amounts of innocent, potentially intimate data, raising serious privacy concerns. A search of a cell phone's text messages might reveal not only communications between co-conspirators but also private text messages unrelated to the crime.").

217. Donohue, *supra* note 40, at 1317 ("[General warrants] turned the concept of innocent until proven guilty on its head. Guilt was presumed, with innocence established only after a search." (footnote omitted)).

218. *See* Carrie Leonetti, *Bigfoot: Data Mining, the Digital Footprint, and the Constitutionalization of Inconvenience*, 15 J. HIGH TECH. L. 260, 297 (2015) ("The difference between data mining and old-fashioned surveillance, however, is not just in the volume of surveillance that can be performed or the amount of information gathered, but also the percentage of surveilled information that is innocent and the consequences of targeting that does not result in either exoneration or prosecution. Because data mining involves combing through information belonging to people about whom the police have no suspicion, in the hope of developing suspicion against one or more of them, it results in people who would have essentially no likelihood of ever being 'tailed' or eavesdropped being monitored without at least the protection of a 'moment of truth' in which the Government either charges them or leaves them in privacy. It has become the ultimate dragnet, and we are now all the usual suspects." (footnotes omitted)).

retrospectively sift through collected data without limit was recognized by Chief Justice Roberts in *Carpenter* as a privacy harm that ran toward everyone in the population.[219] The fact that the retrospective nature of the exploratory search capabilities could be directed both against the target but also anyone else troubled the Supreme Court as a form of government overreach. Again, without limits, this type of rummaging power raises the concern that police will just sift through personal data using one suspicion to justify a more expansive search.

3. Intrusion into Constitutionally Secured Interests

Rummaging involves intrusions into constitutionally secured spaces and interests. In articulating rummaging as a harm, the Supreme Court has identified a practical and substantive concern about government agents intruding on constitutionally secured places, property, or people.[220] As has been identified in the trespass cases (*Jones* and *Jardines*), one part of this intrusion is decidedly physical. Governmental physical intrusion with the intent to gather information is a clear Fourth Amendment harm.[221]

The intrusion harm is not simply a physical invasion, however, but also informational. One way to think about why the Fourth Amendment secures persons, homes, papers, and effects from unreasonable intrusions is to think about the information coming from those areas or things.[222] As I have written before, "informational security" is the core to understanding Fourth Amendment protections.[223] Thus, underlying the Founders' concern about rummaging was a fear of unchecked governmental intrusion into information arising from private places, matters, and things.[224]

---

219. *See* Carpenter v. United States, 585 U.S. 296, 312 (2018).

220. This focus, of course, comes from the textual protections of "persons, houses, papers, and effects" in the Fourth Amendment. U.S. CONST. amend. IV.

221. United States v. Jones, 565 U.S. 400, 404–05 (2012) ("We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."); Florida v. Jardines, 569 U.S. 1, 5 (2013) ("When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'" (quoting *Jones*, 565 U.S. at 406–07)).

222. *See* James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 667 (1985) ("The constitutional text, structure, and history, as well as early fourth amendment cases, support the conclusion that the main reason for constitutionalizing informational privacy is its *instrumental* role as a medium within which other rights and interests can survive, even flourish.").

223. *See* Matthew E. Cavanaugh, *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 MINN. L. REV. 2443, 2467 n.148 (2021) ("*Carpenter* embraces the 'informational security' theory of the Fourth Amendment." (citing Ferguson, *supra* note 20, at 604 (defining "informational security" as "personal information that is secured in some manner from governmental intrusion"))).

224. Byrd v. United States, 584 U.S. 395, 402–03 (2018) ("Few protections are as essential to individual liberty as the right to be free from unreasonable searches and seizures. The Framers made that

As one obvious example, the Fourth Amendment protects homes, not simply because of a physical attachment to real property but because of the private information generated from family and personal activities in the home.[225] Homes are the source of private ideas and activities and are protected because of the things that are created in that space.[226] Property rights are important, of course, but the protection of the home is really about the things that happen inside those four walls, not the walls themselves.[227]

Similarly, with tangible things, the reason the Fourth Amendment originally protected "effects" was not solely because of the value of personal property but also because of the symbolic and religious value of those personal objects.[228] It was what those effects said about the owner, not the things themselves, that needed to be secured against governmental intrusion.[229] Remember, at the time of the Founding, people had far fewer belongings than they do today, so what they owned had more symbolic value. Personal effects were limited to culturally significant markers or

---

right explicit in the Bill of Rights following their experience with the indignities and invasions of privacy wrought by 'general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence.' Ever mindful of the Fourth Amendment and its history, the Court has viewed with disfavor practices that permit 'police officers unbridled discretion to rummage at will among a person's private effects.'" (citation omitted) (first quoting Chimel v. California, 395 U.S. 752, 761 (1969); and then quoting Arizona v. Gant, 556 U.S. 332, 345 (2009))).

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

226. *See* Payton v. New York, 445 U.S. 573, 589–90 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: 'The right of the people to be secure in their . . . houses . . . shall not be violated.'" (quoting U.S. CONST. amend. IV)).

227. Property was not actually mentioned in the Fourth Amendment. Madison's first draft of the Fourth Amendment read:

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

NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 100 n.77 (1937) (quoting 1 ANNALS OF CONG. 452 (1789)). *But see* David E. Steinberg, *The Original Understanding of Unreasonable Searches and Seizures*, 56 FLA. L. REV. 1051, 1077 (2004) ("[A] House of Representatives Committee changed the phrase 'and their other property,' to the narrower language 'effects.'" (citing H. COMM. OF ELEVEN REP. (July 28, 1789), *reprinted in* THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 223–24 (Neil H. Cogan ed., 1997))).

228. *See* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 990 (2016).

229. *See* Ferguson, *supra* note 20, at 606 ("The sparse Founding Era literature suggests a focus on protecting objects which revealed something about the owner—religion, culture, status, or family associations. Searching and seizing a colonist's religious objects was not offensive simply because it interfered with property rights, but because searching revealed personal information about family and faith." (footnote omitted)).

religious items and utilitarian household objects.[230] As Professor Molly Brady has recognized, the Founding generation was concerned about the government interfering with these religious or culturally significant items that related to identity.[231] By searching or seizing a family's effects, the government could also uncover private and religious beliefs and activities.[232] It was not the cast iron pot that was to be secured but the religious icon that was to be protected from government intrusion.

Third, persons were to be secured from police intrusion. At the Founding this was a very physical fear with the prospect of arbitrary arrest and imprisonment a recent memory.[233] While common law policing was quite different than policing today, the Fourth Amendment was written to protect against abuses of police authority against people.[234] In more modern times, of course, the protection of "persons" has also run to the information from those people—be it blood draws, urine samples, or DNA.[235] In both cases, the protection of persons was an attempt to secure people against unwarranted police intrusion into bodily autonomy.

Finally, papers and the ideas contained therein were to be protected against intrusion.[236] As has been detailed, the main harm identified in *Boyd*, *Wilkes*, and *Entick* was governmental intrusion into personal papers.[237] Of course, it was the content of the papers not the physical parchment that mattered.[238] The informational security ran toward the words and ideas, not

230. *See, e.g.*, IVOR NOËL HUME, A GUIDE TO THE ARTIFACTS OF COLONIAL AMERICA 28–30 (1969) (detailing how colonial homes did not have many objects except for basics like pottery, furniture, gun parts, clocks, lamps, and clothing).

231. Brady, *supra* note 228, at 990.

232. Ferguson, *supra* note 20, at 606 ("Rummaging through bedroom drawers was not solely about the inviolate nature of property but, as the early history suggested, also about revealing information that might be contained in those drawers. Interpreted one way, the protection of effects has largely been the protection of what the personal effects revealed or contained."); Crocker, *supra* note 206, at 179 ("A government that invades the home crosses a boundary from the profane to the sacred. As an institution the home has a status on a higher level than ordinary property or social arrangements.").

233. This memory of arbitrary police use of force has remained a part of American law enforcement to the present day. *See generally* PAUL BUTLER, CHOKEHOLD: POLICING BLACK MEN 59–61 (2017); ALEX S. VITALE, THE END OF POLICING (2017).

234. *See* Jules Epstein, *"Genetic Surveillance"—The* Bogeyman *Response to Familial DNA Investigations*, 2009 U. ILL. J.L. TECH. & POL'Y 141, 149–50 (discussing how the search of a person has evolved from physical searches to genetic searches).

235. *See, e.g.*, Schmerber v. California, 384 U.S. 757, 767–72 (1966).

236. Dripps, *supra* note 63, at 52 ("The Fourth Amendment refers to 'papers' because the Founders understood the seizure of papers to be an outrageous abuse distinct from general warrants. The English courts and resolutions of the House of Commons condemned both abuses distinctly.").

237. *See supra* notes 38–51, 66–70 and accompanying text.

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

the form of how those ideas were written down.[239] Three justifications have emerged about why personal papers[240] (and the information contained therein) might be protected from government intrusion. The first involves the private nature of ideas and thoughts.[241] Allowing the government to rummage through writings looking for incriminating evidence undermines free expression and free thought.[242] The second is that at the time of the Founding, ideas, creations, and expressions (that might find their way into papers) were considered a form of property to be protected.[243] Influenced

239. *See* Schnapper, *supra* note 36, at 869–70 ("[M]ore than a dozen decisions over the course of a century reiterated that an individual's private papers were absolutely exempt from seizure, regardless of the existence of an otherwise valid warrant." (footnote omitted)).

240. *See* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 211 (2018) ("The Fourth Amendment lists 'papers' expressly, and its authors relied in large part upon the English court precedent affording papers nearly absolute protection." (footnotes omitted)).

241. *See* Bradley, *supra* note 64, at 480–81 ("The most private matters are one's own thoughts and the physical embodiment of those thoughts in the form of communications solely to oneself. These would include a diary, a reporter's notes of an interview or of a news event, and a doctor's tape recording of his or her thoughts and diagnoses following examination of a patient. Such matters, as long as they are not passed to another to read or transcribe, are nothing less than the record of one's own thinking and should be considered as private as the thoughts themselves. Whether they are kept for personal or business reasons is irrelevant. It is the individual's expectation of privacy which is at issue, not a judgment as to the nature of the thoughts." (footnotes omitted)).

242. Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945, 986 (1977) ("A record of one's private beliefs and emotions tells a good deal about the person. Similarly, when one intimately and privately shares such thoughts and feelings with others he reveals much of the inner person he is. Such experiences may include the exchange of letters, tapes, or phone conversations as well as actual gathering and conversation. Just as recognition of the relationship between private reflection, socialization, and personality has led the Court to block legislative attempts to control intimate private conduct, interference with the private life by search or subpoena should be proscribed under the fourth and fifth amendments rather than tolerated as a necessary incident of criminal law enforcement. The privacy value should not suffer abridgement simply because there is reason to believe a person is involved in criminal activity." (footnotes omitted)); *see also* Warden v. Hayden, 387 U.S. 294, 321 (1967) (Douglas, J., dissenting) ("The full privacy protected by the Fourth Amendment is, however, reached when we come to books, pamphlets, papers, letters, documents, and other personal effects. . . . By reason of the Fourth Amendment the police may not rummage around among these personal effects, no matter how formally perfect their authority may appear to be. . . . That is the teaching of *Entick v. Carrington*, *Boyd v. United States*, and *Gouled v. United States*."); Crocker, *supra* note 206, at 210 ("When law enforcement rummages through the contents of a person's library in order to discover grounds for an obscenity prosecution . . . there is a notable similarity to foundational Fourth Amendment English cases when crown officials searched personal papers looking to find evidence for seditious libel prosecutions. These searches tread upon constitutional protections for freedom of speech, which includes the freedom to possess and consume the reading and viewing materials used to spread ideas." (footnote omitted)).

243. Professor Morgan Cloud has artfully argued that modern courts have failed to see the content of private papers as a form of valuable property to be secured because they have forgotten the Enlightenment concept that property included liberties, rights, and the product of labor (including expressive labor). Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 37–38 (2018). Professor Cloud concludes: "Madison emphasized that the most important kinds of property government must protect were not tangible things, but rather a person's thoughts, opinions, and rights." *Id.* at 49.

by the ideas of John Locke[244] who influenced James Madison's draft of the Fourth Amendment,[245] papers were considered a form of "dearest property."[246] The third reason involves the reality that, as a practical matter, police are hard pressed to find incriminating materials in papers without also reviewing other information in the papers.[247] The nature of searching documents is almost always intrusive to other ideas and papers (akin to the overreach concerns discussed earlier).

In sum, the Fourth Amendment mentions specific constitutional interests because of the information contained therein. In addition, these textually rooted informational privacy interests have been augmented with locational privacy interests.[248] The Supreme Court in *Carpenter* and *Jones* explicitly added locational privacy (at least from long-term tracking) to the type of constitutional interests protected by the Fourth Amendment. As discussed, these cases were not just about the act of tracking, but about the informational security eroded as a result of that tracking. Police rummaging is harmful because it intrudes on this informational security around these protected constitutional interests.

---

244. *Id.* at 45 ("Locke wrote famously that a man's property is '*his life, liberty and estate*.' This definition was not a mistake or merely a rhetorical flourish. It was central to his arguments justifying the creation of both private property and societies. Indeed, Locke argued that the ultimate reason people abandon the freedom of nature and accept the constraints inherent in living in society, is '*for the mutual preservation of their lives, liberties and estates, which I call by the general name, property*.'" (footnote omitted) (quoting JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT §§ 87, 123 (C.B. MacPherson ed., Hackett Publ'g Co. 1980) (1690))).

245. *Id.* at 47–48 ("Madison's definition of property is similar to Locke's. If anything, Madison expresses the Lockean theories of property—both broad and narrow—more clearly than had Locke. Madison described the narrow theory of property as 'that dominion which one man claims and exercises over the external things of the world, in exclusion of every other individual,' and listed 'land, or merchandize, or money' as examples. Madison also espoused a grander definition of property, which was more important than material possessions. 'In its larger and juster meaning, it [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*.'" (footnote omitted) (quoting 6 JAMES MADISON, *Property*, *in* THE WRITING OF JAMES MADISON 101 (Gaillard Hunt ed., 1906))).

246. Dripps, *supra* note 63, at 61 ("History suggests that certain 'effects'—private 'papers'—were indeed originally understood to deserve more constitutional protection than others.").

247. United States v. Bennett, 409 F.2d 888, 897 (2d Cir. 1969) ("The reason why we shrink from allowing a personal diary to be the object of a search is that the entire diary must be read to discover whether there are incriminating entries; most of us would feel rather differently with respect to a 'diary' whose cover page bore the title 'Robberies I Have Performed.' Similarly, the abhorrence generally felt with respect to 'rummaging' through the contents of a desk to find an incriminating letter would not exist in the same measure if the letter were lying in plain view."); *see also* Schnapper, *supra* note 36, at 899.

248. State v. Jean, 407 P.3d 524, 526 (Ariz. 2018) ("GPS tracking may constitute a search for Fourth Amendment purposes if its use involves a common law trespass or invades a person's reasonable expectation of privacy." (citations omitted) (first citing United States v. Jones, 565 U.S. 400 (2012); and then citing Katz v. United States, 389 U.S. 347 (1967))).

4. Exposure

A fourth harm arising from police rummaging involves public exposure of private information and the resulting embarrassment. Rummaging through a house or papers or personal effects means the threat of exposing the "privacies of life" to others in the community.[249] The public nature of investigation involves the possibility of damaging reputations and dignity interests through the raw assertion of power by government agents over individuals.[250] Rummaging, thus, includes the power to intimidate and humiliate via the threat of public exposure of private facts as a mechanism of governmental social control.

Both at the time of the Founding and the present day, rummaging damages reputations.[251] One of the consequences of the government rummaging through houses was that the event identified the person as a suspect of a crime to neighbors and the community. Suspicionless (or even suspicious-based) targeting of a person marks the person as connected to criminal activity. Even if nothing is found in the search, and even if no prosecution results, the reputational harm of a public search inflicts its own damage.[252]

Exposure also raises concerns about the chilling nature of possible surveillance to silence dissent or gain political advantage.[253] This point is important because it connects back to First Amendment principles. The original power and goal of government rummaging was to stifle political

249. *See* Steven Duke, *Making* Leon *Worse*, 95 YALE L.J. 1405, 1419 n.104 (1986) ("A home search can inflict embarrassment or pain on the searchees . . . .").

250. Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1255 (2012) ("When the police search for evidence of crimes, they implicitly (or explicitly) accuse the person of a crime and subject the person to domination, coercion, and force, as well as to embarrassment and humiliation.").

251. Donohue, *supra* note 40, at 1318 ("American legal scholars later agreed with Parliament that 'even when conducted in the discreetest [sic] manner,' the execution of a general warrant 'might injure the most virtuous in their reputation and fortune.' While, alone, it may not suffice to create a right to seize innocent people, such an instrument could nevertheless 'throw in the way of messengers a temptation to inquire into the life and character of persons.'" (quoting HERBERT BROOM & GEORGE L. DENMAN, CONSTITUTIONAL LAW VIEWED IN RELATION TO COMMON LAW, AND EXEMPLIFIED BY CASES 608 (Maxwell & Son 2d ed. 1885))).

252. Interestingly, state cases cabined the Supreme Court's holding in *California v. Greenwood*, 486 U.S. 35 (1988) (allowing police rummaging through trash), by explicitly placing restrictions to prevent embarrassment and the indignity that would come with such a public search. The Montana Supreme Court, for example stated, "officers cannot openly rummage through a person's garbage at the curb or in the alley, to the embarrassment or indignity of the owner." State v. A Blue In Color, 1993 Chevrolet Pickup, 116 P.3d 800, 805 (Mont. 2005) (citing Litchfield v. State, 824 N.E.2d 356, 363 (Ind. 2005)).

253. *See* Donohue, *supra* note 40, at 1317 ("[The power given by rummaging and general warrants] was vulnerable to abuse. The government could use the instrument against citizens to prevent political opposition, to consolidate economic or political control, or to stifle ideas contrary to those held by government officials." (footnote omitted)).

dissent.[254] The sedition that led to the *Wilkes* and *Entick* prosecutions raised issues of political speech and associational liberty.[255] Rummaging to silence dissenting voices is, thus, a long-standing Fourth Amendment harm.[256] The threat to expose critical voices using police search powers lies at the heart of a concern about rummaging.

5. Rummaging as Harm

As has been discussed in this Section, four distinct harms can be identified as emerging from the Fourth Amendment's history and doctrine to center the concern of rummaging. The harms overlap and intersect and are not always consistent, but each one speaks to a particular type of concern. Simply put, there is something wrong—constitutionally wrong—about the government having the ability to intrude in an arbitrary and overreaching manner that threatens to expose information from a constitutionally protected interest. It is not that the actions necessarily involve trespass or a violation of a reasonable expectation of privacy, but something different: they raise the distinct harm of rummaging.

The next Section takes this insight and attempts to provide a framework for future analysis. Police actions that fail the rummaging test will be deemed unreasonable searches under the Fourth Amendment.

B. The Rummaging Test

The rummaging harms discussed above exist both in the physical world and the digital world. The costs are real and offer a counterweight to the benefits of government access to the incriminating data.

The rummaging test offers a way to analyze contested police actions. Judges should ask whether the harms discussed in Section II.A, are present. More specifically, courts should ask whether a police action involves: (1) arbitrary enforcement of police power; (2) overreaching exploratory expansions of initially justified searches; (3) intrusions into constitutionally secured interests (e.g., homes, persons, papers, effects, location); or (4) exposure of private details as a form of political or social control. If any

254. *See id.*

255. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 249, 252–54 (2016) ("[I]n light of the history and purpose of the Fourth Amendment, it is fair to say that 'papers' should be read to protect expressive and associational data, regardless of its form, how it is created, or where it is located.").

256. Donohue, *supra* note 40, at 1318–19 ("Beyond the collection of private or embarrassing information, giving the government insight into one's private affairs raised the potential that information obtained could be used as leverage. It could be made public to defame political adversaries. Even without criminal penalties, it could harm an individual's reputation and standing in the community. The Founders sought to protect against information being misused in this way.").

of those harms are present, then the Fourth Amendment is implicated, and if not sufficiently mitigated by a warrant or other limiting principle, then the police action should be considered unreasonable.

To be clear, the rummaging test applies to the initial threshold search question and the overarching reasonableness question. The questions raise different considerations, but both embrace the core harm of rummaging.

1. The Rummaging Test as a Threshold Test

For the threshold question of whether the Fourth Amendment applies (i.e., whether the police action was a "search"), the rummaging test adds a new consideration to the analysis beyond reasonable expectations of privacy or physical trespass. Namely, courts should ask: was the information obtained via police rummaging?—meaning in a manner that creates the harms (arbitrariness, overreach, intrusion, exposure) described above. If so, like a reasonable expectation of privacy test[257] or trespass test,[258] this intrusion will constitute the kind of government act that implicates the Fourth Amendment.

Note two things. First, the questions about whether a government action is arbitrary, overbroad, intrusive, or exposing are different than the question of whether a reasonable expectation of privacy was violated. Some police actions will be protected by the Fourth Amendment that would fall outside of the two existing tests. As will be discussed, police searches of trash might both be considered rummaging and yet not violate a reasonable expectation of privacy or be a trespass search. Second, just because the Fourth Amendment is implicated does not mean that there was a Fourth Amendment violation. The threshold test just identifies the types of harms the Fourth Amendment can address.

2. The Rummaging Test and Reasonableness

For the ultimate question of reasonableness, courts would ask whether the rummaging harms described above were mitigated in a way to counteract those harms. The most obvious way to avoid the rummaging problem is to craft protections to address arbitrariness, overreach, intrusion, and exposure. Warrants have long played this role. A well-designed warrant—even one targeting private information—acts as its own anti-rummaging principle. In fact, one way of conceptualizing the warrant requirement itself is to view it as a direct response to the harm of rummaging. This logic tracks the warrant exception cases where the initial

257. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
258. United States v. Jones, 565 U.S. 400, 409 (2012).

justification permits a limited search that is specific, particularized, and conducted in a manner that restrains extraneous rummaging.[259] Of course, even with a warrant, if the rummaging harms have not been mitigated, police acquisition of information may run afoul of the Fourth Amendment.

3. The Rummaging Test and Existing Fourth Amendment Doctrine

Because background principles involving rummaging have long influenced Fourth Amendment law, many of the seminal Fourth Amendment cases will come out the same way applying this new test. As discussed, most of the traditional Fourth Amendment canon involved limited searches with basic technology and did not raise these rummaging harms.[260] Similarly, most searches based on particularized warrants do not run afoul of the rummaging test.[261]

Some cases, however, come out differently. Take, for example, *California v. Greenwood*—the case involving the search of the defendant's trash.[262] *Greenwood* asked the question of whether police investigators sifting through a suspect's trash was a Fourth Amendment search. It is hard to get more concrete about the realities of rummaging when literal rummaging is central to the case. In *Greenwood*, the Court ignored the privacy harms of rifling through one's trash, stating that there was no reasonable expectation of privacy in abandoned property.[263] Mr. Greenwood put his trash out to be collected and never expected it back, thereby extinguishing or abandoning any privacy claim to its contents.[264]

Applying the rummaging test, however, suggests a different answer because a different set of harms is emphasized. First, the practice evinced an arbitrary power without limits or oversight. After all, under the government's argument, anyone's trash can now be searched under the theory that this act does not require a warrant or probable cause. Second, the search was overbroad. Police were not just looking for direct evidence of drugs (the drugs were not going to be in the trash) but other inferences of drug dealing—seeking out other unknown, possibly incriminating evidence a step removed from the instant case. Third, the examination of the trash intruded on intimate and private matters coming from a constitutionally protected place (a home and its effects). The trash was from the home and

259. The search incident to arrest exception is a good example. *See* Logan, *supra* note 108, at 381–84.

260. *See* Dripps, *supra* note 63, at 50–51.

261. The particularized nature of the warrant would limit arbitrariness, overreach concerns, private intrusion fears, etc.

262. California v. Greenwood, 486 U.S. 35, 37–38 (1988).

263. *Id.* at 40–41.

264. *Id.* at 39–40.

revealed information from the home. Finally, there is even an element of embarrassment and public exposure in the nature of the search (of the trash), not to mention the possibility of discovering evidence of other innocent family members outside the target of the search.[265]

The rummaging test, thus, adds a protection beyond the reasonable expectation of privacy, asking whether the government should have this power to root around in our trash without constitutional limits. In finding there were rummaging harms, a court could determine that the Fourth Amendment was implicated in the government's actions.

Secondarily, the rummaging test asks whether the harms are such that a court should find the police action unreasonable. The response to any rummaging harm, of course, is to get a particularized and narrowly drawn warrant.[266] A warrant detailing what was being searched for—e.g., drugs or drug paraphernalia—could respond to some of the concerns about particularity and the capture of other innocent, unrelated persons. In other words, had the Supreme Court applied the rummaging test in *Greenwood*, the warrantless police actions would be deemed a Fourth Amendment search and without a warrant unreasonable. Yet, with a warrant that addressed the rummaging harms, however, the same police action might not have been considered to violate the Fourth Amendment (under this rummaging theory).

A rummaging focus becomes even more clarifying in the recent digital surveillance cases. Specifically, in *Carpenter* and *Riley*, one can see the important role the rummaging test can play in the analysis.[267] As discussed, *Carpenter* is a threshold search case involving whether the police acquisition of location data was a Fourth Amendment search because of the personal details potentially revealed.[268] *Riley* is a search incident to arrest case focusing on a warrantless search of a smartphone.[269] Again, both of these cases offer good examples of how the Supreme Court has embraced—without necessarily acknowledging it—the principles behind the rummaging test.

---

265. As mentioned, for this reason two state courts have placed limits on police trash searches to limit this embarrassment and exposure. *See supra* note 252 and accompanying text.

266. Responses to mitigate rummaging harms might include: (1) limiting such grants of power by identifying a particularized area, place, thing, or data source to examine; (2) minimizing the scope of the search to avoid collecting information outside the specific and particularized justification, thereby avoiding incidental collection of non-targets' data; and (3) obtaining information in a way that avoids intimidation (physical, political, or expressive), thereby reducing the physical and chilling impacts of government surveillance. A government agent's course of conduct that generates any of these harms (without appropriate mitigation) could be deemed unreasonable under the rummaging test.

267. *See* Carpenter v. United States, 585 U.S. 296, 303 (2018); Riley v. California, 573 U.S. 373, 399 (2014).

268. *See Carpenter*, 585 U.S. at 302–03.

269. *See Riley*, 573 U.S. at 378.

Carpenter demonstrates why a rummaging test belongs in the foreground of Fourth Amendment search analysis. Again, police were searching through millions of data points for information connecting Timothy Carpenter to the robberies. The harms in *Carpenter* have less to do with expectations of privacy in our phone data as they do with the government's power to rummage through everyone's digital lives without a warrant. After all, as Justice Kennedy recognized in dissent, the privacy expectations of an individual cellphone owner might not run to the third-party phone provider tracking his location. To make a cellphone work, the company needs to track the device, and most consumers expect the phone to work and thus be tracked. While we all might be dependent on the third-party digital service to function in the world, what reasonable expectations exist about such ubiquitous, inescapable technologies is less clear.

Yet, looked at from the perspective of police power to rummage through that locational data without a warrant, the harms are clear. The idea that police could track everyone and comb through the digital trails to connect the dots about anyone without limits is arbitrary and invasive. The power to sift through the collective travel details of anyone and everyone is a significant personal liberty harm that infringes on how we use our personal property (our phones). Issues of power, dignity, and privacy arise from that location data, and freedoms involving a person's association, dissent, and autonomy are threatened by exposure. The point is simply that, by bringing the rummaging harms to the foreground, Chief Justice Roberts's concerns about the arbitrary and indiscriminate aggregation of data, the risk of retrospective searching, the creation of persistent surveillance systems, and the exposure of the privacies of life makes a lot more sense. In other words, had Chief Justice Roberts recognized the salience of rummaging, the majority would not have had to work so hard to rethink reasonable expectations of privacy.

Applying the rummaging test to *Riley* also shows why a warrantless search of a smartphone is unreasonable. Almost all the harms are evident. First, remember what happened in the case. Police found a gun in Riley's car after a traffic stop and, in an effort, to find corroborating incriminating evidence, police searched through his smartphone's photos and found evidence of his involvement in a shooting. Again, the photos were not connected with the initial justification for the arrest, were obtained without a warrant, and required police sifting through the contents of the entire phone.

The harms thus encompass sorting through the content of digital papers, contacts, calls, texts, emails, calendars, and photos. Everything that would have been in Wilkes's or Entick's studies would be on Riley's phone. As Chief Justice Roberts recognized, the data in the smart phone was probably

more revealing than the content in a modern home.[270] The information comes from an effect, raising concerns of intruding on private information from our constitutionally secured things, but goes well beyond the personal to also include associational freedoms (location data), expressive labor (communications and thoughts), valuable personal information (with monetary value), and hints about political interest and activities. The power to search and the scope of the information available were not limited in any particularized way, with no minimization steps taken, and what police found was only indirectly connected to the gun possession crime they were initially investigating. If conceived as the police power to search any digital device recovered incident to arrest, the harms would involve arbitrary searches of personal photos or contacts with a real potential to expose embarrassing details on the target and all of their contacts. Such searches would be both overbroad compared to the justifications for search incident to arrest (officer safety/destruction of evidence) and also quite chilling to freedoms because any arrest (no matter how minor) might result in the search of all of our mobile data collected on a smartphone.[271] Also, of course, innocent people who simply communicated with Riley would have been caught up in the net of suspicion.

The rummaging test can be applied to a host of new surveillance challenges currently being evaluated solely against the reasonable expectation of privacy test (or, less commonly, the trespass test). The rummaging test adds clarity to all of them. In the next Part, I focus on two of these new digital policing challenges that can be addressed using the rummaging test: (1) smart-home data, and (2) long-term digital pole cameras.

III. THE RUMMAGING TEST APPLIED TO DIGITAL POLICING

As has been demonstrated, rummaging is a historically rooted and doctrinally consistent principle in Fourth Amendment analysis. The rummaging test is not meant to replace existing Fourth Amendment tests but to augment those tests to highlight the harm of law enforcement rummaging. This Part will show why rummaging is a helpful heuristic for courts evaluating the reasonableness of digital surveillance. By focusing on two emerging digital policing problems that are ill-suited to traditional Fourth Amendment analysis, the hope is to show how an emphasis on the harms of digital rummaging can clarify the doctrine.

---

270. *Id.* at 396–97.

271. A remedy to the rummaging harm might have involved a specific, particularized warrant looking only for evidence of the guns actually recovered in the initial arrest. Anything else would likely be the type of expansive, exploratory search frowned upon by the Founding generation.

The examples discussed below—(1) data from smart homes, and (2) long-term digital pole cameras—both present difficult Fourth Amendment questions arising from data collection inside and around the home.

A. Smart Data from Smart Homes

Smart sensors in thermostats, refrigerators, and speakers are rewiring our expectations of privacy in the home.[272] Smart devices can answer your questions, turn off the lights, and add efficiencies by mapping the patterns of your daily routine.[273] The Internet of Things has turned dumb effects into smart objects with a promise of consumer convenience at the mere cost of your personal data.[274] The problem is that those smart devices are also always surveilling you.[275]

Because smart sensors can reveal personal data from the inside of a home, police are beginning to recognize the evidentiary value of smart devices.[276] In a few previous articles, I have addressed how the Internet of Things and the growth of smart devices opens the door for new forms of police investigation inside a home.[277] For example, in a murder case with an Amazon Echo in the home, police may seek to discover if any recordings were made.[278] "Echo, how do you remove bloodstains?" might be good circumstantial evidence to prove culpability in a murder investigation. Smart devices like smartwatches and video cameras have also been used as

272. *See* Ferguson, *supra* note 1, at 819–20; *see also* Bronshteyn, *supra* note 1, at 459–60.

273. *See* Mary Ellen Callahan, *Connected Homes and the Curtilage*, 18 N.C. J.L. & TECH. 1, 5 (2016) ("The sensors and the smart homes are looking for ways to save money, looking for patterns and ways to improve your quality of life along with non-obvious relationships.").

274. *See, e.g.*, Tomer Kenneth, *Personalization of Smart-Devices: Between Users, Operators, and Prime-Operators*, 70 DEPAUL L. REV. 497, 499, 504 (2021); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98 (2014) (describing the data collected by the Internet of Things).

275. *See, e.g.*, *Counting Every Moment*, ECONOMIST (Mar. 3, 2012), www.economist.com/node/21548493 [https://perma.cc/CZU9-6E7M].

276. *See* James O'Toole, *Cops Can Access Your Connected Home Data*, CNN BUS. (June 16, 2014, 2:25 PM), https://money.cnn.com/2014/06/16/technology/smart-home-footage/index.html [https://perma.cc/SWK2-ASSU].

277. *See* Andrew Guthrie Ferguson, *Digital Habit Evidence*, 72 DUKE L.J. 723, 756–58 (2023) (discussing criminal evidence introduced under Federal Rule of Evidence 406).

278. *See* Flynn, *supra* note 6; Eliott C. McLaughlin & Keith Allen, *Alexa, Can You Help with This Murder Case?*, CNN BUS. (Dec. 28, 2016, 8:48 PM), http://edition.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html [https://perma.cc/MXD2-LSCJ].

evidence in criminal cases.[279] Whether they undermine an alibi or clarify the timing of an event, digital clues are present in smart data from the home.[280]

Most of this smart data is mediated through privately owned third-party providers (Amazon, Google Nest, SimpliSafe, etc.) raising hard questions about expectations of privacy of home data that is also collected and held by private companies.[281] For example, the Google Nest system stores data in the home devices and in a Nest cloud service.[282] The Amazon Ring doorbell camera stores images at the home and on Ring servers.[283] Accessing the information directly from the house device would require a probable cause warrant under a traditional Fourth Amendment analysis, but what about the third party's data? The Supreme Court has not yet determined whether a warrant is required to obtain the smart-home data from a private third-party provider.[284] The question brings up whether the "third-party doctrine" survives *Carpenter* and related claims about the expectations of privacy one might have in data handed over to private third

279. *See* Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance*,*'* 9 U.C. IRVINE L. REV. 635, 638 (2019) ("[L]ocation information can be vital for pinning down a suspect to a crime scene or providing them with an alibi. Indeed, real-time and historical geolocation data has become a common piece of evidence collected in criminal investigations.").

280. *Husband Sentenced to 65 Years in Fitbit Murder Case*, AP NEWS (Aug. 18, 2022), https://apnews.com/article/shootings-597c5b876c1f7de77fcde24621ec5e94 [https://perma.cc/H8HD-XAEM]; Erin Moriarty, *21st Century Technology Used to Help Solve Wisconsin Mom's Murder*, CBS NEWS (Oct. 20, 2018, 10:30 PM), www.cbsnews.com/news/the-fitbit-alibi-21stcentury-technology-used-to-help-solve-wisconsin-moms-murder [https://perma.cc/DD83-PUSP]; Cleve R. Wootson Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story.*, WASH. POST (Feb. 8, 2017, 6:15 AM), www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-froma-burning-house-his-pacemaker-told-police-a-different-story [https://perma.cc/3Q84-L8WB]; *Amazon's Alexa May Have Witnessed Alleged Florida Murder, Authorities Say*, LOCAL3NEWS (Mar. 23, 2022), www.wrcbtv.com/story/41263095/amazons-alexa-may-havewitnessed-alleged-florida-murder-authorities-say [https://perma.cc/6M9N-64U9]; Rafael Olmeda, *Alexa, Is He Guilty of Murder? Amazon Device May Have Heard Slaying, Cops Say*, S. FLA. SUN SENTINEL (Oct. 31, 2019, 6:57 PM), www.sun-sentinel.com/news/crime/flne-amazon-alexamurder-investigation-20191031-qccpvdl6kng5hcx3z6eusxa264-story.html [https://perma.cc/8KCW-QUY5].

281. Caleb Garling, *Google's Purchase of Nest Gives It Entree into Homes*, SFGATE (Jan. 13, 2014), https://www.sfgate.com/tech/article/google-s-purchase-of-nest-gives-it-entree-into-5139771.php [https://perma.cc/WF3R-7UA9] ("Palo Alto's Nest is a flagship brand in the burgeoning Internet of Things—a catchphrase for a wave of tech innovations that could turn once-mundane appliances like ovens, thermostats, microwaves, fridges and garage-door openers into a network of devices that communicate with each other.").

282. Nur Lalji, *Featurization and the Myth of Data Empowerment*, 15 WASH. J.L. TECH. & ARTS 1, 14 (2019) ("Nest's Learning Thermostat . . . provides users with insight into 'their own data trail' by allowing them to see what information it has gleaned about a user's daily routine.").

283. *See, e.g.*, Evan Selinger & Darrin Durant, *Amazon's Ring: Surveillance as a Slippery Slope Service*, 31 SCI. AS CULTURE 92, 92 (2021).

284. *Carpenter* suggests that such a warrant would be required if the data was the type of data that revealed the privacies of life, which presumably home device data would reveal. *See also* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 525 (7th Cir. 2018) (finding smart-home meter readers a search under *Carpenter*).

parties.[285] In prior writings, I have argued how the reasonable expectation of privacy test should apply to smart data from a home and why a warrant should be required,[286] but—in truth—how the Supreme Court might rule on the issue remains an open question.[287]

This Article focuses on a different issue, namely how the rummaging test clarifies the Fourth Amendment harms and avoids the third-party doctrine problem. Take, for example, a hard case involving a man who allegedly murdered his wife in their home. The murder suspect will not give permission for direct access to the data from the physical devices. Yet, police wish to request data from each of the smart devices (e.g., Echos, smart light sensors, video doorbells, and other smart objects in the home) because police believe they might be able to track the murderer's path as he went about the killing and the coverup, and perhaps find other incriminating clues. The next Section applies the rummaging test to show why (at a minimum) a warrant is required for third-party data stored about the individual. The argument here is that, even if courts find no reasonable expectation of privacy and no physical intrusion (trespass), there is still a cognizable Fourth Amendment argument to protect this third-party data from government acquisition.

1. Rummaging and the Smart Home

Before applying the rummaging test, it is important to step back and see what police are doing in these kinds of investigations. Police know that a crime has occurred. They hope, but do not know for certain, that always-listening smart sensors in the home will provide clues for their investigation.[288] They have probable cause that a crime has occurred but not necessarily probable cause that the smart devices hold clues to that crime (it is a hunch). The desire is to search through the recorded data in the hopes of generating additional clues helpful for the case. In other words, police

---

285. *See generally* Harvey Gee, *Last Call for the Third-Party Doctrine in the Digital Age After* Carpenter*?*, 26 B.U. J. SCI. & TECH. L. 286, 300 (2020); Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1058 (2019).

286. To oversimplify a complicated subject, my argument is that police need a warrant to obtain information from inside a home. Physical searches have long required a warrant. But even in the context of digital searches, whether police are recording elevated heat levels or intercepting content from a computer, to access the data located in a home, courts (generally) have required a probable cause warrant. *See* Ferguson, *supra* note 1, at 879–80.

287. In addition, there is no physical trespass inquiry with smart data from smart homes because the information is being obtained via digital means through the third party.

288. *See* Arielle M. Rediger, *Always-Listening Technologies: Who Is Listening and What Can Be Done About It?*, 29 LOY. CONSUMER L. REV. 229, 231 (2017); *see also* Sapna Maheshwari, *Hey, Alexa, What Can You Hear? And What Will You Do with It?*, N.Y. TIMES (Mar. 31, 2018), www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html [https://perma.cc/H69F-NMWF].

wish to sift through the stored home data in the hopes that some of it might be incriminating, knowing most of it will be innocent, embarrassing, or irrelevant. Independent of any reasonable expectation of privacy or trespass question, this should be considered digital rummaging, raising many of the harms discussed earlier.[289]

First, warrantless collection of smart-home data raises arbitrariness concerns. As a power, it would mean that police could collect all third-party data on any house for any reason (without a warrant or even a murder investigation). If the Fourth Amendment does not apply to such actions, police could essentially convert surveillance doorbells into police cameras,[290] voice assistants into wiretaps,[291] and video cameras into spying devices[292] (not to mention knowing when you exercised,[293] got a good night's sleep,[294] or used the bathroom).[295] If no warrant is required, police could collect the data for any purpose including using it for political embarrassment or other petty grievances. While it is most likely that police would restrict their investigations to serious criminal activity, without a warrant requirement they would not be so limited. Once smart devices become commonplace, it will become relatively easy to use the sensors to target a wider group of people or disfavored individuals.

The overreach problem also exists as almost everything in the home might be revealed with enough digital access to smart devices. No matter the original justification, the additional rummaging might open up a new set of unrelated crimes and/or embarrassing personal information. The collection of intimate details could be easily weaponized to embarrass[296] or

289. *See infra* Section II.A.

290. *See* Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 6:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach [https://perma.cc/B58E-NGLT].

291. *See* Lindsey Barrett & Ilaria Liccardi, *Accidental Wiretaps: The Implications of False Positives by Always-Listening Devices for Privacy Law & Policy*, 74 OKLA. L. REV. 79, 92–96 (2022).

292. *See* Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 100 (2017) ("IOT security cameras permit owners to remotely view security feeds and control the devices through a mobile application or a website without a physical video system.").

293. *See* Nikolina Ilic, *Could Your Peloton Be Spying on You?*, WOMEN'S HEALTH AUSTL. (June 21, 2021), www.womenshealth.com.au/could-your-peloton-be-spying-on-you [https://perma.cc/H8PA-4S73].

294. *See* Brenda Stolyar, *Google's New Nest Hub Tracks Your Sleep and It Feels Very Judgy*, MASHABLE (Mar. 30, 2021), https://mashable.com/review/google-nest-hub-sleep-tracking-review [https://perma.cc/GZB8-6VA2].

295. *See* Navin Bondade, *The New AI Toilets Will Scan Your Poop to Diagnose Your Ailments*, TECHGRABYTE, https://techgrabyte.com/ai-toilets-scan-poop-diagnose-ailments [https://perma.cc/XGF4-RACL].

296. *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1942–44 (2019) (discussing privacy harms of sexually embarrassing facts).

expose a political enemy.[297] All of these arguments show how a rummaging analysis highlights the Fourth Amendment harms of obtaining smart-home data without a warrant.[298]

Third, the requested data intrudes on private space and personal information created from inside the house.[299] Homes are core Fourth Amendment spaces, and as Justice Scalia once opined, everything in the house should be protected for Fourth Amendment purposes.[300] The smart-home data thus reveals personal details that would otherwise not be obtainable absent an entry into the home (if then).[301] From a rummaging perspective, the third-party ownership of the data does not matter. Police are still intruding on information that came from a home—the most protected of constitutional spaces.

Finally, of course, everyone in the house—not just the target—will have their data collected. This secondary overreach problem means children, spouses, friends, and visitors might lose privacy protections merely by being proximate to the target. No matter how focused the suspicion, the smart devices will reveal information about the extended set of familial and social connections, many of whom will be innocent.

The conclusion that warrantless access to smart devices runs afoul of the rummaging test aligns with analysis of smart-home protection under the reasonable expectation of privacy test.[302] Both recognize that this protected information should require a probable cause warrant. A judge applying the rummaging test in lieu of the other threshold search tests could find that such digital rummaging implicates the Fourth Amendment. Note, again, however, that if rummaging is a standalone Fourth Amendment threshold test, it does not matter how the court rules on reasonable expectations of privacy. Rummaging can still offer Fourth Amendment protection.

---

297. Finally, devices themselves might be endangered as the police would be interfering with the property interests of the physical sensors. All of these harms point to the need for a warrant to limit the arbitrary enforcement and minimize rummaging impacts.

298. Even with a warrant, one can imagine Lord Camden railing against a government power that could expose personal family details on the pretext of looking for some possible treasonous activity.

299. United States v. Karo, 468 U.S. 705, 716 (1984) ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.").

300. Kyllo v. United States, 533 U.S. 27, 37–38 (2001) (recognizing that all details of the home are protected, intimate or not).

301. The revelation of personal details from inside a home that could not have been observed without technology was the Supreme Court's test for a search in *Karo*. *See* 468 U.S. at 715 ("The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant.").

302. Or at least this has been my argument in previous work. *See* Ferguson, *supra* note 20, at 631 (discussing how warrantless collection of smart data should be considered a search).

As will be discussed in the next Section, police can still obtain this information, just with a warrant. The rummaging harms can be remedied with a carefully crafted warrant for information from particular devices for which investigators have probable cause that information will be present. The harms of rummaging can be mitigated by responding to the specific harms.

2. Warrants and Smart-Home Data

Based on the above argument, particularized warrants should be required for the data from smart-home devices and/or stored by third-party providers. Yet, even with a warrant, police must address the rummaging harms. For example, an unparticularized warrant or an overbroad search into incidental or innocent smart-device data might still create rummaging harms. In other words, even with a signed warrant, digital rummaging amongst home data might be considered constitutionally unreasonable.

For example, a judicial warrant for all the smart data from all the devices in a house would raise rummaging problems. Courts applying the rummaging test should ask whether the rummaging harms—arbitrariness, overreach, intrusion, and exposure—were appropriately mitigated. As an example, a warrant that did not address minimization about innocent individuals living in the house or did not narrowly limit the collection time to a particular moment relevant to the crime might still run afoul of the rummaging principle. Perhaps a warrant might allow the acquisition of information from a smart-home camera to see who left the home the night of the murder but not the smart bed to see how it was used the month before. In other words, a strong argument can be made that, even with evidence that a crime had occurred (murder) and a signed warrant (probable cause of the murder), police would still be precluded from obtaining some private, personal details arising from living in a smart home that involved rummaging for additional incriminating clues. If the warrant were restrictive enough to not be a backdoor attempt to rummage for other evidence, the acquisition of digital information might be allowed.

Note that such a limitation on police investigative power is new—and one that exists in tension with traditional practice.[303] In a traditional murder case, a probable cause warrant would allow the search of an entire house for physical objects that might be connected with the crime.[304] The probable

303. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1248 (2010) (discussing the differences between traditional searches and searches of digital information).

304. *See* United States v. Ross, 456 U.S. 798, 821 (1982) ("[A] warrant that authorizes an officer

cause of the crime would justify the mere possibility (the hunch) that additional corroborative evidence might be present somewhere in the house. This search might even include the seizure of electronic storage devices like computers or tablets or phones.[305] As long as a judicial officer signed off on the paperwork, there would be little recourse for challenging the unreasonableness of the government's actions.[306]

The rummaging test changes the analysis, reflecting the more originalist protection of homes and personal papers that were more zealously guarded against police rummaging.[307] Sifting through smart-home data in the hopes of uncovering incriminating information is akin to searching through private papers in the hopes of finding private incriminating ideas.[308] While not technically physical papers, the digital equivalents are memorialized records revealing of our thoughts, questions, and intimate practices. There is little difference between a written diary recording the time you went to sleep each night and the automated digital equivalent of your smart mattress. Both reveal the "privacies of life."[309]

Simply stated, the rummaging test would not give a free pass to a search even with a lawful warrant but would require an additional reasonableness inquiry about whether the rummaging harms had been adequately addressed. Specific probable cause for specific data from specific digital devices in the home would be required to address the rummaging harms.

B. Long-Term Digital Pole Cameras

In the last few years, sophisticated long-term digital pole camera systems have created challenges for courts trying to balance Fourth Amendment rights and police investigators' need for evidence just outside the home.[310]

---

to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. A warrant to open a footlocker to search for marihuana would also authorize the opening of packages found inside.").

305. *See generally* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 98 (2005) (discussing the rules around digital searches for digital evidence).

306. Of course, police might need to obtain a second warrant to search through electronic storage devices. *See id.* at 98–101.

307. *See supra* notes 74–75 and accompanying text.

308. *See, e.g.*, Commonwealth v. McCarthy, 142 N.E.3d 1090, 1099 (Mass. 2020) ("The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants. Just as police are not permitted to rummage unrestrained through one's home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modern society.").

309. Carpenter v. United States, 585 U.S. 296, 305 (2018).

310. *Compare* United States v. Trice, 966 F.3d 506, 516–20 (6th Cir. 2020), United States v. May-Shaw, 955 F.3d 563, 567–69 (6th Cir. 2020), *and* United States v. Cantu, 684 F. App'x 703, 704–06 (10th Cir. 2017), *with* Commonwealth v. Mora, 150 N.E.3d 297, 313 (Mass. 2020), People v. Tafoya, 494 P.3d 613, 622–23 (Colo. 2021), *and* United States v. Houston, 965 F. Supp. 2d 855, 898 (E.D. Tenn. 2013).

Long-term pole cameras involve digital video camera systems attached to physical poles or structures that continuously monitor a particular location.[311] The camera systems can record for months at a time.[312] The goal from a law enforcement perspective is to watch the home and environs in the hopes that incriminating details will emerge from the hours of surveillance data.

For example, in *United States v. Tuggle*, the Seventh Circuit Court of Appeals faced a Fourth Amendment challenge to the warrantless use of a digital pole camera system that monitored Travis Tuggle's home for eighteen months straight.[313] The technology at issue involved three cameras and generated a dataset of stored video footage that was searchable and connected to other law enforcement data systems. Investigating officers could search through the footage, identify people, and watch the outside of Tuggle's home whenever they wished.[314] Over the course of eighteen months, everyone who was present around Tuggle's home found themselves caught in the surveillance footage.[315] Dozens of contacts proved useful enough to be evidence in Tuggle's drug distribution prosecution.[316]

Tuggle moved to suppress the evidence arguing that the video system was a search for Fourth Amendment purposes that violated his reasonable expectation of privacy without a warrant.[317] An openly conflicted Seventh Circuit Court expressed concern with the growing surveillance state being created by new technologies but eventually held that Tuggle had no reasonable expectation of privacy in his movements and activities outside his home.[318] The court reasoned that the activity was exposed to the public,

311. Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 17–19 (2020) (describing police use of pole cameras).

312. For example, in *Tuggle*, the cameras were on for eighteen months. United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021) ("Together, the three cameras captured nearly eighteen months of footage by recording Tuggle's property between 2014 and 2016.").

313. *Id.*

314. *Id.* ("The government installed three cameras on public property that viewed Tuggle's home. Agents mounted two cameras on a pole in an alley next to his residence and a third on a pole one block south of the other two cameras. The first two cameras viewed the front of Tuggle's home and an adjoining parking area. The third camera also viewed the outside of his home but primarily captured a shed owned by Tuggle's coconspirator and codefendant, Joshua Vaultonburg.").

315. Appellant's Brief & Appendix at 21–22, United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021) (No. 20-2352) ("Although the pole cameras were stationary, the cameras monitored everything in the vicinity of Mr. Tuggle's residence. The Government was able to use the cameras to determine Mr. Tuggle's habits, such as when he left and returned to his residence.").

316. *Tuggle*, 4 F.4th at 511–12 ("The officers tallied over 100 instances of what they suspected were deliveries of methamphetamine to Tuggle's residence.").

317. *Id.* at 512.

318. Judge Flaum writing for the majority was quite explicit in his concern about increasing surveillance technologies. *Id.* at 509 ("[W]e are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans. Foreseeable expansion in technological capabilities and the pervasive use of

and the Supreme Court had not protected collection of information available to public observation.[319] Similar cases have been litigated in other federal and state courts.[320]

All of the long-term digital pole camera cases were decided under a reasonable expectation of privacy analysis because that, of course, is the current controlling Fourth Amendment test. As a result, courts asked whether the defendant had a reasonable expectation of privacy in the publicly observable areas of their property. In answering the question, "no," several courts relied on cases like *Knotts*, generalizing about expectations around being observable in public.[321] The tenor of the *Tuggle* decision, however, voiced concern about growing power of technological surveillance, suggesting something is missing in the Fourth Amendment analysis. I argue that the missing consideration is rummaging.

1. Rummaging and Long-Term Digital Pole Cameras

Under the rummaging test, courts would evaluate the pole-camera surveillance by looking at the harms involved. With digital pole cameras, all four of the identified rummaging harms are present (arbitrariness, overreach, intrusion, and exposure). The analysis below suggests that rummaging harms show that a long-term pole camera is a Fourth Amendment search and an unreasonable one without a particularized warrant.

First, the arbitrariness harm is present. The enforcement power—unlimited by law, regulation, policy, or judge—means that police can conduct pole camera surveillance anywhere and against anyone at any time. Knowing such a power exists may have chilling effects on those who wish to criticize government power or just those who wish to live free from government monitoring. Even if focused just on Mr. Tuggle, the lack of time limits, content restrictions to minimize incidental collection, or any other rule or policy about what could be collected about a life, is rather arbitrary. At least as a constitutional matter, there was no limit to the years data could be collected by those cameras or the other sources of information that could be added to the collection. Aggregating all of a person's home visitors,

---

ever-watching surveillance will reduce Americans' anonymity, transforming what once seemed like science fiction into fact."). Yet, despite these misgivings, the court upheld the use of the cameras under the Fourth Amendment. *Id.* at 511 ("In short, the government's use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment.").

319. *Id.* at 514–15 (citing United States v. Knotts, 460 U.S. 276, 282 (1983)) (arguing that cameras as mere enhancements did not violate a reasonable expectation of privacy).

320. *See supra* note 310; *see also* United States v. Moore-Bush, 36 F.4th 320, 321 (1st Cir. 2022).

321. *Tuggle*, 4 F.4th at 514–15 (citing *Knotts*, 460 U.S. at 282) (arguing that cameras as mere enhancements did not violate a reasonable expectation of privacy).

activities, and personal patterns for years opens up a risk of arbitrary abuses of government power to sift through the information to find incriminating facts.[322]

The overreach harms are also present. While Tuggle and other suspected drug dealers do not make sympathetic figures, the reality is that police were not limited to investigating just the suspected drug deals. Anything Tuggle did would be captured. In many cases, the goal of pole camera surveillance is not necessarily to prove what was known but to collect more evidence not yet known. Without particularized limits of what could be observed or used as evidence, anything Tuggle did that was captured on camera could become evidence for this case or other cases. Equally troubling, anything anyone who visited Tuggle did could become evidence. The video surveillance encircled everyone in Tuggle's orbit. Family, friends, innocent neighbors, delivery people, and co-conspirators all are captured on video. If any of them were involved in a criminal act the suspicion directed against Tuggle could be redirected toward them.

Third, there was an intrusion into one of the express constitutional interests identified in the Fourth Amendment.[323] Here we have a home with information from the curtilage of that home being collected without a warrant. Homes are constitutionally protected areas.[324] From the Founding era on, curtilage counted as part of a home because so many of the intimate and family activities of the home happened just outside the home.[325] Whether we were talking about intimacy around outhouses, bathing, or just outdoor leisure activities, the area around the home was to be secured from governmental intrusion.[326] In the *Tuggle* case, the surveillance intruded upon personal details about Tuggle's home life—what he did, when he did it, who he did it with, and even what he did not do (like leave the house). For months, cameras revealed private details of his family life.[327] There is

322. *See* Ferguson, *supra* note 9, at 50–53 (discussing why *Tuggle* was incorrectly decided).

323. The harms of rummaging are not limited to the specific Fourth Amendment interests of home, person, papers, or effects, but those do offer clear examples of what is protected. At a minimum, the textually referenced areas and interests should gain enhanced Fourth Amendment protection.

324. Crocker, *supra* note 206, at 177 ("The home occupies a central place within Fourth Amendment jurisprudence.").

325. *See* Collins v. Virginia, 584 U.S. 586, 592–93 (2018) ("[T]he Fourth Amendment's protection of curtilage has long been black letter law. '[W]hen it comes to the Fourth Amendment, the home is first among equals.' . . . 'The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened.'" (first quoting Florida v. Jardines, 569 U.S. 1, 6 (2013); and then quoting California v. Ciraolo, 476 U.S. 207, 212–13 (1986))).

326. *See* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1313–16 (2014) (discussing the history and law of curtilage).

327. United States v. Tuggle, 4 F.4th 505, 511–12 (7th Cir. 2021) ("Camera footage depicted individuals arriving at Tuggle's home, carrying various items inside, and leaving only with smaller versions of those items or sometimes nothing at all.").

little debate that private information coming from the home and curtilage was revealed through the cameras, even if it might not be considered a violation of a reasonable expectation of privacy or a trespass with the intent to gather information.

Finally, independent of the inculpatory information obtained about Tuggle's life, police also obtained embarrassing information—including the time Tuggle apparently urinated in his front yard.[328] The embarrassment of exposure pales in comparison to how police can use the evidence in a felony drug-distribution trial but does raise concerns about how such information could be used to discredit reputation or silence an individual who might be critical of the government. Mr. Tuggle had more important things to worry about than reputation, but for other people subject to long-term video surveillance, these personal revelations might prove quite damaging.

The point is that the harms decried by the rummaging principle are present in the pole camera surveillance whether or not a reasonable expectation of privacy in public is violated. For a year and a half, police collected information about all of the people, patterns, practices, and personal activities of Tuggle and his family hoping that some of that activity might be incriminating. Further, they stored the data in a searchable dataset (connected to additional police data) in a way that allowed for retrospective searching for particular actions.[329] Both real-time and retrospective monitoring allowed police to sift for corroborating incriminating details in a very generalized manner. This type of digital rummaging should be considered a Fourth Amendment search and unreasonable without a warrant.

2. Warrants and Long-Term Digital Pole Cameras

The fact that the rummaging principle is implicated in long-term pole camera surveillance does not mean it should be forbidden. Cameras can still play a role in police investigations.[330] However, the analysis does suggest that the harms of rummaging should be mitigated. A narrow judicial warrant—especially a warrant with minimization requirements, time limits, or other considerations—could mitigate some of the rummaging concerns. For example, if police believe a suspect is involved in drug dealing, a

328. Appellant's Brief & Appendix at 21–22, United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021) (No. 20-2352) ("The pole cameras were also deployed to observe and record Mr. Tuggle walking outside in his boxers and urinating in his front yard, amongst other private activities.").

329. *Tuggle*, 4 F.4th at 511 ("While officers frequently monitored the live feed during business hours, they could later review all the footage, which the government stored at the Federal Bureau of Investigation office in Springfield, Illinois.").

330. *See* Carpenter v. United States, 585 U.S. 296, 316 (2018) ("We do not . . . call into question conventional surveillance techniques and tools, such as security cameras.").

particularized request to observe for a limited time (and minimizing the rest) might well be reasonable if safeguards are put in place to avoid overbroad collection. Taking the rummaging harm seriously would mean creating particularized limits and reducing concerns about arbitrary enforcement. Again, in shifting the focus away from expectations of privacy and toward protections against rummaging, a different Fourth Amendment value is elevated and a different set of actions is protected.

CONCLUSION

The Fourth Amendment was born in response to government agents rummaging for personal information. The rummaging harms involved arbitrary, overbroad intrusions, which exposed personal information and threatened the security of private spaces, people, papers, and things. This Article has sought to bring that background rummaging principle into the foreground to show why it provides a better understanding of Fourth Amendment protections in the digital age.

As has been detailed, digital surveillance only imperfectly fits expectations of privacy because we are reliant on third parties to provide digital conveniences. Everything digitized can be stored and shared by those third parties and thus is available to police with legal process. Further, third-party digital mediators complicate traditional understandings of expected privacy because, in a digital age, almost everything connects through private third parties that run the digital infrastructure. Physical trespass questions are also unavailing when considering a purely digital world without any actual physical need to interfere with physical property to obtain the data. Neither of the traditional theories of Fourth Amendment protection fit the digital age, suggesting a need for something new.

At the same time, the harms of government intrusion into private information have only increased. Massive datasets from geofence technologies,[331] reverse-keyword searches,[332] automated license plate readers,[333] and a host of AI technologies[334] will allow for increased digital

331. *See generally* Brian L. Owsley, *The Best Offense Is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 HOFSTRA L. REV. 829, 838 (2022); Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512 (2021) ("Geofence warrants rely on the vast trove of location data that Google collects from Android users—approximately 131.2 million Americans—and anyone who visits a Google-based application or website from their phone, including Calendar, Chrome, Drive, Gmail, Maps, and YouTube, among others." (footnotes omitted)).

332. *See* People v. Seymour, 536 P.3d 1260, 1275 (Colo. 2023) (discussing reverse-keyword searches).

333. *See* Commonwealth v. McCarthy, 142 N.E.3d 1090, 1097–106 (Mass. 2020) (discussing automated license plate reader (ALPR) searches).

334. *See* Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, WASH. POST (Apr. 2, 2021, 9:00 AM), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ [https://perma.cc/PP9S-66QA].

rummaging. The ability of police to examine our digital lives for clues is a power that needs a constitutional counterweight. The rummaging principle provides a historically rooted response to government search power. The rummaging test seeks to expose and check the ability of government actors to sift through the digital trails of life for incriminating clues. As demonstrated in the examination of smart-home data and digital pole cameras, the rummaging test provides a more apt analysis of why digital surveillance is harmful and how the Fourth Amendment can be responsive to those harms.

The goal of this Article is to unearth and expose the harms of digital rummaging in the hopes that the concept can enrich Fourth Amendment theory. The anti-rummaging principle has been core to the Supreme Court's Fourth Amendment understanding without it ever taking center stage. Perhaps in a world awash in data, the rummaging principle can act as a constitutional counterweight to balance security and privacy in the digital age.