VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2022 UNIVERSITY OF VIRGINIA VOL. 25, NOTE 1

A Dignitary Fourth Amendment Framework and Its Usefulness for Mobile Phone Searches

CAMERON CANTRELL†

† J.D., University of Washington School of Law (expected June 2022); B.S., Worcester Polytechnic Institute (2019). Many thanks to Professor Mary Fan for her advice and encouragement through all stages of this work's development, and to VJOLT's editorial team for helping this work become its best self. In all other regards, I thank my mother Bethan for her life-long teachings of compassion and self-determination.

ABSTRACT

The Fourth Amendment is often described—sometimes lovingly—as a mess. Beginning as a concept of personal rights so closely held as to incite revolution, the fifty-four words comprising the Amendment have left much of search and seizure law up to the imagination of the country's scholars and jurists. The resulting incoherence, compounded and exacerbated by the common law, is ill-suited to keep up with (or even stay in the same race as) searches aided by modern technologies. This Note proposes an original Fourth Amendment framework that distills the jurisprudential noise into a simple melody, written in terms of the personal dignitary interests each search implicates. Part I retraces the path of Fourth Amendment caselaw along a hidden continuum that the caselaw has long tracked. Part II sifts through the legal and practical realities of mobile phone searches to place such searches on that continuum, ultimately between searches of the home and searches of the body. Part III builds on the arguments presented in Parts I and II to advocate for mobile phone searches being designated *sui generis*, deserving of their own treatment, in Fourth Amendment law.

TABLE OF CONTENTS

INTRODUCTION

Fourth Amendment jurisprudence is widely regarded as a mass of doctrinal puzzles and complexities. Its noise comes at great cost to common law development. Scholars and jurists alike arrive at conflicting conclusions and digital technology continues to advance at a yet-unmatchable pace. Law enforcement searches of mobile phones in particular are increasingly common, but the courts' response is lagging far behind.

In the few years since the Supreme Court applied the warrant requirement to mobile phone searches, many have sought to calibrate the remarkably unique qualities phones hold with existing Fourth Amendment caselaw. Sophisticated police technologies have turned this exploration into a more pressing mission, but courts have not found an answer. I introduce an original Fourth Amendment framework derived from the dignitary interests the Fourth Amendment protects, then apply it to demonstrate why mobile phone searches should be designated *sui generis* in Fourth Amendment jurisprudence.

I. THE FOURTH AMENDMENT PROTECTIONS AGAINST UNREASONABLE SEARCHES FALL ON A CONTINUUM MEASURED IN DIGNITARY INTERESTS.

In Part I, I identify a novel pattern in the Fourth Amendment's jurisprudence. Rather than relying on the gestated, sometimes incoherent body of Fourth Amendment rules that have made its adaptation to modern technologies painful at best, I lay out the evolution of its fifty-four words to illuminate that it has always operated to preserve personal dignitary interests. I revisit doctrinally significant caselaw to demonstrate that the Fourth Amendments protections against a search are always proportionate to the dignitary interests implicated. I further define this continuum in formulaic terms for the mathematically inclined among us. Lastly, I describe how new types of searches can be placed on the continuum to easily understand the Fourth Amendment's protections across different searches.

A. *The Fourth Amendment is a Shifting Puzzle*

Like every other Amendment in the Bill of Rights, the Fourth Amendment began as a reaction to the circumstances of the colonies. Most significantly, it reacted against the colonial "writs of assistance," which British customs inspectors used to perform dragnet searches of any place smuggled goods *might* be concealed.[1] Notably, the Fourth Amendment was written before police existed in the form they take today.[2] "Our colonial forebears could not have predicted the sheer numbers of law enforcement agents at work today, the breadth of their operational mandate, or their pervasive authoritarian presence. . . . If the Framers . . . *had* foreseen the shape of modern law enforcement, they undoubtedly would have recognized the substantial dangers that it poses to liberty" in the language of the Fourth Amendment.[3] Instead of being intentionally designed as a police restriction, then, the Fourth Amendment originated as a set of personal rights so strongly held as to incite revolution.[4] Read this way, it reflects the observation that "the human personality deteriorates and dignity and self-reliance disappear where homes, persons and possessions are subject at any hour to unheralded search and seizure by the police."[5]

---

[1] *See, e.g.*, discussion in Riley v. California, 573 U.S. 373, 403 (2014) ("[T]he 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"); discussion in Payton v. New York, 445 U.S. 573, 583, n.21 (1980) ("[T]he hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of British tax laws"); G. M. Leasing Corp. v. United States, 429 U.S. 338, 355 (1977) ("[O]ne of the primary evils intended to be eliminated by the Fourth Amendment was the massive intrusion on privacy undertaken in the collection of taxes pursuant to general warrants and writs of assistance").

[2] *See, e.g.*, discussion in Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 830–32 (1994).

[3] *Id.* at 837 (emphasis in original).

[4] *Riley,* 573 U.S. 373, 403 ("Opposition to such searches was in fact one of the driving forces behind the Revolution itself").

[5] *Brinegar v. United States*, 338 U.S. 160, 180–81 (1949) (Jackson, J., dissenting).

"The course of true law pertaining to searches and seizures . . . has not—to put it mildly—run smooth."[6] Upon first impressions of modern policing, the Supreme Court determined that the Fourth Amendment guarded property interests, so its protections required government intrusions resembling common law trespass ("actual physical invasion").[7] Over the following years, however, as the discussion around the constitutional scope of a right to privacy progressed,[8] the Court softened its tone. Shortly after using the Fourth Amendment to condemn a search where government trespass was not present,[9] the Court identified a constitutional right to privacy in the "penumbra" of several Amendments in the Bill of Rights—including the Fourth Amendment.[10]

The Court gradually sidled away from its narrow reading, guiding the development of Fourth Amendment remedies to enable "protection of privacy . . . without regard to proof of a superior property interest."[11] This expanded Fourth Amendment reading came to a head in *Katz v. United States*,[12] where the Court definitively found that the Fourth Amendment's protections "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[13] Instead, the

---

[6] *Chapman v. United States*, 365 U.S. 610, 618 (1961) (Frankfurter, J., concurring).

[7] *Olmstead v. United States*, 277 U.S. 438, 466 (1928).

[8] *See* discussion in *Griswold v. Connecticut*, 381 U.S. 479, 510, n.1 (1965) (Black, J., dissenting) ("The phrase 'right to privacy' appears first to have gained currency from an article written . . . in 1890 which urged that States should give some form of tort relief to persons whose private affairs were exploited by others. . . . some States have passed statutes creating such a cause of action, and in others state courts have done the same thing by exercising their powers as courts of common law"). *See generally* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 INDIANA L. J. 549, 560, n.52–57 (1990).

[9] *Silverman v. United States*, 365 U.S. 505, 512 (1961) (finding a search via eavesdropping did not technically involve common law trespass).

[10] Griswold v. Connecticut, 381 U.S. 479, 484 (1965). *See also* William M. Beaney, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212, 215 (1962) ("[t]he nearest thing to an explicit recognition of a right to privacy in the Constitution is contained in the Fourth Amendment").

[11] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 307 (1967).

[12] 389 U.S. 347 (1967).

[13] *Id.* at 353.

Fourth Amendment must be read to protect a person from searches that invade their reasonable and personal expectations of privacy.[14]

The *Katz* test dominated Fourth Amendment jurisprudence for several decades. More recently, though, in *United States v. Jones*,[15] the Court revived the trespass test as an alternative to the *Katz* test, finding that a search involving government trespass is sufficient (but not necessary) to trigger Fourth Amendment protections. This happens when the government "physically occupie[s] private property for the purpose of obtaining information."[16] The Court has since employed the modern trespass test to identify Fourth Amendment searches, without relying on the *Katz* test, multiple times.[17]

The zig-zagging development of Fourth Amendment law between *Katz*'s reasonableness test and *Jones*'s trespass revival has resulted in a "doctrinal incoherence . . . [that] disturbs many judges and scholars."[18] More than 200 years of common law evolution has seen courts "heap[] solution upon solution without troubling [them]selves with the task of discovering a basic, understandable theme" connecting each Fourth Amendment case to the rest.[19] To muddle the waters further, much of this piecemeal growth has involved circumstances that the

[14] *Id.* at 361 (Harlan, J., concurring).

[15] 565 U.S. 400 (2012).

[16] *Id*. at 404–05.

[17] *See generally* Florida v. Jardines, 569 U.S. 1 (2013); Grady v. North Carolina, 575 U.S. 306 (2015).

[18] David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 J. CON. L. 581 (2008).

[19] Steven C. Douse, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J. L. REFORM 154, 155, n.7 (1972) (quoting M. C. SLOUGH, PRIVACY, FREEDOM AND RESPONSIBILITY 91–92 (1969)).

Amendment's authors could not have considered,[20] and sometimes in the face of Circuit splits.[21]

With criminal trials marching on anyway, apathetic to this confusion, "[t]he importance of distilling a rational and understandable body of rules out of a complex maze of conflicting judicial precedents cannot be overestimated."[22] Judges must wade through the complex body of Fourth Amendment law *and* the extensive bodies of scholarship attempting to interpret that law.[23] They are then tasked with striking a balance of a flexible rule of law that can be adapted to particular facts but avoids becoming dysfunctional.[24]

Even if there is no single trick of logic to "make all of the decisions of the [Supreme] Court in this area perfectly consistent,"[25] we still must achieve "some assurance that the cases are being decided in accordance with a coherent analytical

---

[20] *See generally* HOUSE COMM. ON THE JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 99-647, at 16 (1986) ("[w]hen the Framers . . . acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into [] 'houses, papers and effects'. . . . During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions"). And as exemplified in searches assisted by twenty-first century technologies, *see, e.g.,* United States v. Forrester, 512 F.3d 500, 503 (9th Cir. 2008) (finding a warrant was not necessary for the government to, via software, monitor websites defendant visited because "Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit").

[21] For example, what amounts to a "search" in the common spaces, such as the hallways, of a private apartment building. *Compare* United States v. Carriger, 541 F.2d 545, 550 (6th Cir. 1976) (holding government intrusion into such a common space can be a search because tenants have a reasonable expectation of privacy therein), *with* United States v. Eiszler, 567 F.2d 814, 816 (8th Cir. 1977) (holding government intrusion into such a common space cannot be a search because tenants do not have a reasonable expectation of privacy therein).

[22] Steven C. Douse, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J.L. REFORM 154, 155, n.7 (1972).

[23] *See* Steinberg, *supra* note 18, at 598, n.99.

[24] Douse, *supra* note 22, at 155.

[25] Wayne R. LaFave, *Warrantless Searches and the Supreme Court: Further Ventures into the "Quagmire"*, 8 CRIM. L. BULL. 9, 27 (1972).

framework."[26] That framework, I believe, is the continuum I posit here.

B. *The Fourth Amendment Protections Guard Dignitary, Not Just Privacy, Interests*

Naturally, the Fourth Amendment protections stewarded by the *Katz* and trespass tests are not absolute.[27] They are simply, in the law's eyes, worth preserving. A search is granted access to the Fourth Amendment's protections if it passes one of these tests,[28] as passage amounts to a legal finding that the search significantly implicates the interests guarded by the Fourth Amendment. Accordingly, the proposed continuum comes into existence if the instant search passes at least one of these tests.

Just as a search does not have to pass both tests to invoke the Fourth Amendment, it does not have to intrude on a specific set of interests; though it must pass at least one test, and it must intrude on a dignitary interest.

Though the Fourth Amendment primarily protects privacy, together with bodily integrity[29] and personal dignity,[30] it ultimately safeguards "dignitary interests."[31] This follows the

---

[26] *Ibid*.

[27] The protections only apply if the search is "unreasonable." U.S. CONST. amend. IV. More conceptually, "[a]ll rights tend to declare themselves absolute to their logical extreme. . . . [but] in fact are limited by the neighborhood of principles of policy which are other than those on which the particular right is founded, and which become strong enough to hold their own when a certain point is reached." Hudson Cnty. Water Co. v. McCarter, 209 U.S. 349, 355 (1908).

[28] Either, or both. *See* United States v. Jones, 565 U.S. 400, 409, 411 (2012) ("[T]he Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test. . . . we do not make trespass the exclusive test"); *see also* Florida v. Jardines, 569 U.S. 1, 12 (2013) (Kagan, J., concurring) (deciding the case on privacy as well as property grounds).

[29] Winston v. Lee, 470 U.S. 753, 761 (1985) (citing Schmerber v. California, 384 U.S. 757, 767 (1966)).

[30] *Schmerber*, 384 U.S. at 767.

[31] *Winston*, 470 U.S. at 761 (discussing "dignitary interests" in terms of personal privacy, bodily integrity, and personal security); *accord* Sims v. Labowitz, 885 F.3d 254, 262 (4th Cir. 2018).

general understanding of privacy as "a part of the more general right to immunity of the person,"[32] and the Fourth Amendment's protections as "founded as much in dignity as in secrecy."[33]This ethos espouses that, as Justice Jackson said, dignity "disappear[s]" without the Fourth Amendment's protections."[34]

The Fourth Amendment's operation as a guardian of dignitary interests is clear in several parts of its jurisprudence. For example, the Fourth Amendment ensures that an individual's privacy rights are "not subject to the discretion of the [particular] official in the field."[35] The discretion must lay, then, with that individual, at least to the extent that the individual is acting objectively reasonably.[36] Further, the Fourth Amendment's "third-party" doctrine recognizes this insofar as mitigating a person's dignitary interests in information the person chooses to share with others.[37] In this perspective, the Fourth Amendment guards a person's inherent autonomy to choose when to publicize themselves and their effects; "the right to [their] personality."[38]

The continuum I posit thus reflects that the Fourth Amendment will guard against an instant search proportionately to how much the search endangers dignitary interests.[39] At one

---

[32] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 207 (1890).

[33] Wilson v. Layne, 141 F.3d 111, 128, n.26 (4th Cir. 1998), *aff'd*, 526 U.S. 603 (1999). *See also* Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019), cert. denied, 140 S. Ct. 937 (2020) (quoting U.S. Dep't of Just. v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person") (internal quotation marks omitted)).

[34] *See* Steiker, *supra* note 2, at 843.

[35] Delaware v. Prouse, 440 U.S. 648, 654–55 (1979) (quoting Camara v. Mun. Ct., 387 U.S. 523, 532 (1967) (internal quotation marks omitted)).

[36] *See* Katz, *supra* note 8, at 554.

[37] *See generally* United States v. Miller, 425 U.S. 435, 443 (1976) (reiterating that a person does not have an expectation of privacy in information they reveal to third parties); *accord.* Smith v. Maryland, 442 U.S. 735, 743–44 (1979). *See also* discussion *infra* text accompanying notes 81–86.

[38] Warren & Brandeis, *supra* note 32, at 207.

[39] In mathematical terms, the continuum is an Archimedean ray on the $(0, \infty^{+})$ x-axis.

end of the continuum—say, the right—are those searches most endangering dignitary interests and afforded the most Amendment protections. At the other end—the left—are searches that pose no meaningful risk, barely invoking the Fourth Amendment.

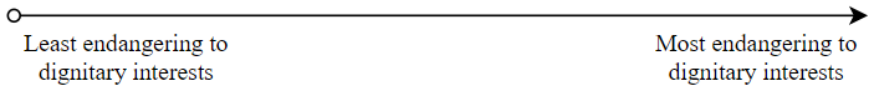

FIGURE 1. The basic continuum.

C. *The Resulting Continuum of Searches*

Whatever intrusion a search entails, the extent and nature of its implications for the dignitary interests determines where on the continuum the search lays. The implications depend on the search's methods and purpose.[40] Consequently, "[a] criminal investigation is generally more intrusive than an administrative or regulatory investigation" because the former "is perceived by the public as more offensive than" the latter in its purpose.[41] Similarly, when someone consents to a government search of a place, the government may only search proportionate to the scope of that consent because the consenter has only abandoned dignitary interests within that scope..[42] When consent is total and unconditional, there are no dignitary interests left for the Fourth Amendment to preserve and the search may be "exhaustive."[43]

The law treats like instances alike, and the Fourth Amendment is no different. Two searches in the same circumstances, like that of a parked car or an abandoned backpack, are treated similarly. These trends correspond to benchmarks on the continuum, though benchmarks are not necessarily absolute. Placement on the continuum may shift case to case, even within the same general type of search. For

[40] Widgren v. Maple Grove Twp., 429 F.3d 575, 584 (6th Cir. 2005) (quoting WAYNE R. LAFAVE, 5 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.1(b) (4th ed. 2004)).

[41] *Id.* at 583–84.

[42] United States v. Thomas, 818 F.3d 1230, 1242 (11th Cir. 2016) (citing United States v. Matlock, 415 U.S. 164, 166–67 (1974)).

[43] *Id.*

example, searches of persons with a diminished expectation of privacy (like those who are arrested,[44] and to a greater extent those who are incarcerated[45]) are scrutinized as if they were further left on the continuum because the law affords those persons fewer dignitary interests.

These considerations are not necessarily the same factors as those bearing on the determination of what is a "reasonable search," *i.e.*, of whether the instant search was respectful of its placement on the continuum. Some searches are categorically reasonable in certain circumstances, hench the useful benchmarks, but the facts may require further balancing to determine it conclusively (for example, if a particular automobile search was reasonable). This distinction is easily illustrated in observing that subjectivity plays a role in what the Fourth Amendment *protects*, but not what the Fourth Amendment *protects from*. For example, a person's subjective expectation of privacy may inform if something is protected by the Fourth Amendment,[46] but an officer's subjective motivation is irrelevant in determining if a search of that thing is unreasonable.[47]

But so long as the Fourth Amendment applies, these shifts will continue to preserve those interests in some measurable way. Body searches at the border, for example, do not recognize the full expectation of privacy that may be realized elsewhere,[48] yet the Fourth Amendment affords protections against those searches based on the "personal indignity suffered by the individual" during the search.[49] Similarly, exceptions to the warrant requirement are limited to the extent that government interests outweigh dignitary interests, restraining

[44] *See, e.g.*, United States v. Robinson, 414 U.S. 218, 235 (1973) (circumscribing the search incident to arrest doctrine).

[45] Bell v. Wolfish, 441 U.S. 520, 557 (1979).

[46] *Katz*, 389 U.S. at 361.

[47] Bond v. United States, 529 U.S. 334, 339, n.2 (2000).

[48] *See infra* note 139.

[49] United States v. Vega-Barvo, 729 F.2d 1341, 1345 (11th Cir. 1984); *accord* United States v. Braks, 842 F.2d 509, 511 n.6 (1st Cir. 1988) ("Invasiveness is a function of the degree of indignity that accompanies a particular search method rather than of the extensiveness or thoroughness of the search per se").

the government's ability to circumvent warrants unless the scales tip their way.[50]

At this point, if you are mathematically minded, you may appreciate a set of nine approximate formulas[51] describing this continuum's framework:

[1] $S := search$,

[2] $\forall\ S :=$ {*search invades space subject has reasonable and personal expectation of privacy in* or *search involves physically occupying subject's private property for the purpose of obtaining information*},

[3] S_{extent}, S_{method}, $S_{purpose}$, S_{nature}, *relevant facts* $\in$ {*dignitary interests*}, *continuum placement* $\in \mathrm{R}^{+}$,

[4] $f_e, f_n, f_p : \{dignitary\ interests^{+}\} \rightarrow \mathrm{R}^{+}$,

[5] $k_r : \{dignitary\ interests\} \rightarrow \mathrm{R}$,

[6] $S_{extent} = f_e(S_{method}, S_{purpose})$,

[7] $S_{nature} = f_n(S_{method}, S_{purpose})$,

[8] $\exists$ *continuum placement* $= f_p(S_{extent}, S_{nature}) \pm k_r$(*relevant facts*), where

[9] *Fourth Amendment protections* $= \gamma$(*continuum placement*), $\gamma: \mathrm{R}^{+} \rightarrow \{dignitary\ interests^{+}\}$.

[50] Terry v. Ohio, 392 U.S. 1, 19 (1968) (noting that search under an exception "must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible") (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)).

[51] As (im)precisely stated as the Fourth Amendment allows, with due effort to avoid the "mechanical" interpretation of the Fourth Amendment rejected by the Supreme Court. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001) (internal quotation marks omitted)).

To state the above formulas in sentences: Where analysis of the instant search indicates the search passes either the *Katz* or trespassory test (or both),[1], [2] then the search's extent, method, purpose, nature, and relevant facts[52] are framed in terms of their relationship to the search subject's dignitary interests, and the search's continuum placement is framed in terms of a positive real number,[3] so distinct placements between searches are more visible. The analyses of the search's extent, method, purpose, nature, and relevant facts are done in terms of affirmative dignitary interests, so the results are measured in terms of their rightward shift on the continuum.[4] In contrast, the analysis of relevant facts can also include mitigating factors, possibly shifting placement to either the right or left.[5] The search's extent and nature both depend on its method and purpose.[6], [7] Therefore, the search has a continuum placement, depending on its extent and nature, adjusting for relevant facts.[8] This placement is proportionate to the protections the Fourth Amendment affords against[53] the search to preserve the search subject's dignitary interests.[9]

D. *Placing Familiar Searches on the Continuum*

This continuum is usefully illustrated through example benchmarks.[54] Recall the less-endangering searches live on the continuum's left end, and the more-endangering searches on its right.[55] Toward the leftmost end are "private" searches, wherein a private party unearths evidence, searches it, then shares it with officers. There, the Fourth Amendment is invoked only if the officer, in their search, exceeds the search conducted by the private party in their own search, as the officer would have further intruded on the subject's dignitary interests.[56] One step to the right are the administrative and regulatory searches,

[52] For example, participation in a parole program, causing diminished dignitary interests. *See infra* notes 170, 189, and accompanying text.

[53] Recall again that this framework does not necessarily include the same factors as those bearing on the determination of what is a "reasonable search," *i.e.*, of whether the instant search was respectful of its placement on the continuum. *See supra* note 27.

[54] *See infra*, Figure 2.

[55] *See supra*, Figure 1.

[56] United States v. Jacobsen, 466 U.S. 109, 117–18 (1984).

afforded only "relaxed" protections that correspond to their minimal intrusion on the subject's interests.[57]

At some point to the right of the "private" search, benchmarks become subject to a warrant requirement (or exception thereof) because those searches implicate dignitary interests fundamental enough to "ensure[] that the inferences to support [their] search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."[58]

As a search nears the continuum's right end, the Fourth Amendment's protections apply more forcefully. Towards this end are searches of the home. Dignitary interests are rooted in the home as a "place of refuge, privacy, and comfort"[59] and as its habitant's "most intimate and familiar space."[60] Accordingly, "the Fourth Amendment has drawn a firm line [requiring a warrant] at the entrance to the house"[61] as well as the land immediately and "intimately tied to the home."[62] Notably, the officer need not physically enter a home for this line to apply; the Fourth Amendment "encompasses searches of the home made possible by ever-more sophisticated technology"[63] when that technology is "not in general public use."[64]

Other dignitary considerations affect the home search's placement. For example, the regular application of the Fourth Amendment's third-party doctrine is slightly weaker in the home, better preserving the privacy interest in information a

[57] *See generally Camara*, 387 U.S.; See v. City of Seattle, 387 U.S. 541 (1967).

[58] *Riley*, 573 U.S. at 382, quoting Johnson v. United States, 333 U.S. 10, 14 (1948).

[59] United States v. Shrum, 908 F.3d 1219, 1232 (10th Cir. 2018), citing United States v. Place, 462 U.S. 696, 703 (1983).

[60] *Jardines*, 569 U.S. at 14.

[61] *Payton*, 445 U.S. at 590.

[62] United States v. Dunn, 480 U.S. 294, 301 (1987).

[63] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 525–26 (7th Cir. 2018), citing *Kyllo*, 533 U.S. at 31–32.

[64] *Kyllo*, 533 U.S. at 40.

person shares with their guest.[65] Similarly, the average nighttime home search is just further right than the average home search, given the heightened indignities involved.[66] This is clearly reflected in procedural rules against nighttime warrant execution.[67]

Several paces down, at the rightmost end of the continuum, is the search of a person's body. The Fourth Amendment gives "significantly heightened protection[s]" to the body compared to property.[68] "Even a limited search of the outer clothing...constitutes a severe, though brief, intrusion upon cherished personal security."[69] While cursory pat-downs are *sui generis* exempted from the warrant requirement,[70] other searches above the body's surface implicate intimate dignitary interests. Urinalysis, for example, is generally considered a search,[71] as is "the taking of a suspect's fingernail scrapings."[72]

Firmly beneath the body's surface, the affected interests are most fundamental. Blood draws, for example, require "a clear indication that in fact [desired] evidence will be found," otherwise the "fundamental human interests require law officers to suffer the risk that such evidence may disappear" in the absence of exigent circumstances.[73] At the continuum's edge is the strip search and visual inspection.[74] There, "[e]ven when

[65] *Wilson*, 141 F.3d at 128, n.15, citing Illinois v. Rodriguez, 497 U.S. 177, 181–82 (1990).

[66] Yanez-Marquez v. Lynch, 789 F.3d 434, 465 (4th Cir. 2015), citing Coolidge v. New Hampshire, 403 U.S. 443, 477 (1971) and Gooding v. United States, 416 U.S. 430, 462 (1974) (Marshall, J., dissenting).

[67] *See* Fed. R. Crim. P. 41(e)(2)(A)(ii) and (e)(2)(C)(ii).

[68] Wyoming v. Houghton, 526 U.S. 295, 303 (1999); *accord Schmerber*, 384 U.S. at 767.

[69] *Terry*, 392 U.S. at 24–25; *accord Houghton*, 526 U.S. at 303.

[70] *See infra* note 167.

[71] Everett v. Napper, 833 F.2d 1507, 1511 (11th Cir. 1987), citing *Schmerber*, 384 U.S. at 767.

[72] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 644 (1989), quoting Cupp v. Murphy, 412 U.S. 291, 295 (1973) (internal quotation marks omitted).

[73] *Schmerber*, 384 U.S. at 770.

[74] Mary Beth G. v. City of Chicago, 723 F.2d 1263, 1272 (7th Cir. 1983), citing *Wolfish*, 441 U.S. at 558 (Marshall, J., dissenting); *accord*

carried out in a respectful manner, and even absent any physical touching, [those] searches are inherently harmful, humiliating, and degrading."[75]

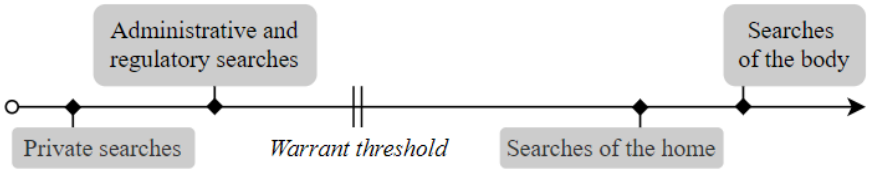

FIGURE 2. Illustrative benchmarks on the continuum.

When courts place a novel search on the continuum for the first time, they consider different factors. Most abstractly, courts first "generally determine whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy, and on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[76]

Courts must also consider the Fourth Amendment's historical roots so that the placement "assur[es] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[77] This degree is indicated in the Fourth Amendment language "prohibit[ing] by name only searches by general warrants. But that was only because the abuses of the general warrant were particularly vivid in the minds of the Framers' generation . . . not because the Framers viewed other kinds of general searches any less reasonable."[78] An example of one such abuse—not anticipated by the Framers, yet still found to have "a close relationship" to the dignitary

Spear v. Sowders, 71 F.3d 626, 634 (6th Cir. 1995) (Jones, J., concurring in part and dissenting in part).

[75] Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 345 (2012) (Breyer, J., dissenting) (internal citation omitted).

[76] *Riley*, 573 U.S. at 385, quoting *Houghton*, 526 U.S. at 300 (internal quotation marks omitted).

[77] *Jones*, 565 U.S. at 406, quoting *Kyllo*, 533 U.S. at 34 (internal quotation marks omitted).

[78] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 669 (1995), citing W. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* (1990) (Ph.D. Dissertation at Claremont Graduate School), at 1554–60.

harms they reviled—is an intrusive search conducted with a biometric facial recognition system.[79]

Recalling that the continuum itself is defined by the Fourth Amendment's trespassory and Katz tests,[80] initial placement naturally involves considering other corollaries of those tests and the broader Fourth Amendment law. For example, jurisprudence recognizes that a person has a lower dignitary interest in what they "knowingly expose[]" to others than what they keep private.[81] This "third-party exposure" doctrine categorically eliminates a person's right to privacy in information they knowingly and voluntarily disclose to others.[82] Relatedly, when a person shares their dignitary interests in the searched thing with someone else, they assume the risk that the other person may expose it to others. Thus they maintain a lesser dignitary interest in the shared thing.[83]

The law, controversially,[84] takes the stance that the party you share information with is a gossip or a spy,[85] and mitigates protections for your dignitary interests accordingly. The third-party exposure doctrine does not extend infinitely, however. A well-known example of this limit is cellular site location information. Considered beyond the doctrine's grasp, such information "implicates privacy concerns far beyond those considered" in the doctrine's seminal cases.[86]

---

[79] *Patel*, 932 F.3d at 1273, quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549, *as revised* (May 24, 2016) (internal quotation marks omitted).

[80] *See supra*, notes 16–27.

[81] *Katz*, 389 U.S. at 351.

[82] *See Miller*, 425 U.S., and *Smith*, 442 U.S.

[83] United States v. Thomas, 818 F.3d 1230, 1242 (11th Cir. 2016) ("[T]he touchstone of the third-party consent rule is assumption of the risk").

[84] *See, e.g.*, *infra* note 160.

[85] *Miller*, 425 U.S. at 443, citing United States v. White, 401 U.S. 745, 752 (1971).

[86] *Carpenter*, 138 S. Ct. at 2220.

II. A SEARCH OF A MOBILE PHONE FALLS BETWEEN A SEARCH OF THE HOME AND A SEARCH OF THE BODY

In Part II, I walk through the many layers of mobile phone searches, including the Fourth Amendment, the enabling technology, and the unique significance of mobile phone searches compared to all other searches. I describe the weighty dignitary interests a person maintains in their mobile phone and compare it to those maintained in their home and their body. I then argue that the search of the mobile phone invades more dignitary interests than the search of a home, but fewer than the search of the body.

A. *A Background on Mobile Phone Searches*

1. The Fourth Amendment Basics

In 2014, the Supreme Court conclusively placed mobile phone searches[87] toward the right end of the continuum in *Riley v. California*.[88] More precisely, the Court placed the search of a mobile phone seized incident to arrest well to the right of the warrant requirement threshold.[89] At the outset of analyzing where on the continuum these searches lay, the Court noted that in *any* search of a cell phone, "the balance between governmental and privacy interests shifts enormously"[90] from

[87] *Riley* did not itself limit what a "search" of a phone could be, but "[t]he searches in *Riley* and its progeny have a common thread – they involve law enforcement officers affirmatively accessing the content within cell phones to gather evidence." United States v. Brixen, 908 F.3d 276, 281 (7th Cir. 2018) (finding that officer did not "search" the phone by texting the phone then viewing the notification on the phone's lock screen), citing United States v. Gary, 790 F.3d 704, 708 (7th Cir. 2015) (finding that operating the phone to determine its number and access its call log was a search) and United States v. Jenkins, 850 F.3d 912, 916 (7th Cir. 2017) (finding that browsing the device's settings to determine its number and accessing its call log was a search).

[88] 573 U.S. 373 (2014).

[89] *Riley*, 573 U.S. at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

[90] United States v. Lichtenberger, 786 F.3d 478, 487 (6th Cir. 2015), citing *Riley*, 573 U.S. at 386.

any analog counterparts. Mobile phone searches implicate personal interests that "add[] weight to one side of the scale while the other [side] remains the same."[91]

The *Riley* Court dealt with the mobile phone's unique situation at length. In the analog world, searches of items seized incident to arrest are on the left end of the continuum. Officer safety and preservation of evidence override the arrested person's dignitary interests. This justification, however, does not "ha[ve] much force with respect to digital content on cell phones."[92] To that end, while the holding is limited to phones seized incident to arrest, the Court notes that the exigent circumstances search of a mobile phone—involving similar interests as the search incident to arrest—will not be easily justified except in rare situations.[93]

The Court emphasizes that modern mobile phones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers[,]"[94] containing "nearly every aspect of [a] li[fe]—from the mundane to the intimate."[95] A search of one, therefore,

> would typically expose to the government far more than the most exhaustive search of a house: a phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[96]

---

[91] *Id.* at 488, citing *Riley*, 573 U.S. at 392–93.

[92] *Riley*, 573 U.S. at 386.

[93] *Id.* at 391 (quoting Missouri v. McNeely, 569 U.S. 141, 153 (2013) ("If the police are truly confronted with a 'now or never' situation,—for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt—they may be able to rely on exigent circumstances to search the phone immediately") (internal quotation marks omitted).

[94] *Id.* at 393.

[95] *Id.* at 395.

[96] *Id.* at 396–97.

This relationship is so intimate that the "proverbial visitor from Mars might conclude [it was] an important feature of human anatomy."[97] A mobile phone search, then, reconstructs "[t]he sum of an individual's private life . . . labeled with dates, locations, and descriptions,"[98] and warrant exceptions must be justified appropriately.[99]

Separate from *Riley*, which asks whether a warrant is required, is the body of cases asking what those warrants must contain. The dragnet general warrants so reviled by the Constitution's Framers present peculiar concerns—many would say worrisome[100]—when the "place" to be searched is simply stated as a certain mobile phone. Phones contain not only an unusually large amount of information compared to the physical "places" traditionally searched, but also a more intimate, descriptive mix of records than would commonly be found in a home,[101] making them "especially vulnerable to a worrisome exploratory rummaging by the government."[102] Warrants for phone searches are often boilerplate and expansive,[103] relying on courts to assume "a reasonable investigation cannot produce a more particular description" under the circumstances and thus "allow a broader sweep."[104] There is no uniform federal rule on

---

[97] *Id.* at 385.

[98] *Id.* at 394, 396.

[99] *See, e.g.*, United States v. Camou, 773 F.3d 932, 942–43 (9th Cir. 2014) (extending *Riley* to the vehicle exception to the warrant requirement on this logic, and further noting that "[w]hereas exigency searches are circumscribed by the specific exigency at hand and searches incident to arrest are limited to areas within the arrestee's immediate control or to evidence relevant to the crime of arrest, vehicle exception searches allow for evidence relevant to criminal activity broadly.")

[100] *See, e.g.*, Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, UPTURN (Oct. 2020), https://www.upturn.org/reports/2020/mass-extraction/.

[101] *Riley*, 573 U.S. at 395 ("Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different.").

[102] United States v. Russian, 848 F.3d 1239, 1245 (10th Cir. 2017) (noting this vulnerability is true of mobile phone searches), quoting United States v. Christie, 717 F.3d 1156, 1164 (10th Cir. 2013) (identifying this vulnerability in computer searches).

[103] Koepke, *supra* note 100 at 50–51.

[104] United States v. Griffith, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (citing Andresen v. Maryland, 427 U.S. 463, 480, n.10 (1976)).

what a digital particularity requirement would look like, leaving courts[105] and scholars[106] alike to arrive at differing conclusions.

Distinct again from those two questions is what happens once the government is "inside" the phone. Prior to *Riley*, there was some discussion that nested-storage data in phones was directly comparable to the containers and sub-containers present in other parts of Fourth Amendment caselaw.[107] *Riley*, however, rejects that premise. As phones "differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person,"[108] applying container jurisprudence equally to the prototypical footlocker and the average mobile phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[109] Such an evenhanded rule would "give police officers unbridled discretion to rummage at will among a person's private effects,"[110] signaling a reigning-in of standard Fourth Amendment doctrine in the context of mobile phone searches.

---

[105] *Compare, e.g.*, *Russian*, 848 F.3d at 1245 (requiring limiting principles such as relevance to specific federal crimes or specific types of materials), *with, e.g.*, *United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (noting that the general rule of giving warrants more latitude on particularity when authorizing searches for contraband items applies to mobile phones).

[106] *Compare* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241 (2010) *with* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1 (2011).

[107] Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and A Primer*, 75 MISS. L. J. 193, 197–200 (2005). *See also* discussion in Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J. L. & TECH. 311 (2010).

[108] *Riley*, 573 U.S. at 393–94 ("Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant . . . rather than a container the size of [a] cigarette package").

[109] *Id.* at 393.

[110] *Id.* at 399 (quoting Arizona v. Gant, 556 U.S. 332, 345 (2009) (internal quotation marks omitted)).

2. The Practical Reality

Setting past judicial philosophy aside for a moment, it is clear that mobile phones implicate unique dignitary interests, and the *Riley* Court's search warrant requirement must be applied in a manner guarding those interests. Application must also honor the fact that mobile phones, and the technologies that the government uses to search them, have steadily increased in prevalence and invasiveness over the last few decades.[111] So, what would this look like? The answer depends on the methods law enforcement use to execute the searches.[112]

Mobile device forensic technologies ("MDFTs") are far and away the most commonly used method for this purpose.[113] MDFTs are a hardware-software combination that lets police search personal phones—even locked ones—by extracting and analyzing a phone's data then organizing it into a sophisticated user interface.[114] This library-like view lets police sort data "by the time and date of its creation, by location, by file or media type, or by source application."[115] Police can even use keywords to search the phone's content, "just like you might use Google to search the web."[116] Law enforcement generally uses MDFTs to retrieve communications and photos but, depending on the MDFT vendor, they can also reach third-party apps and "deleted" data, as well as discover the precise operations a phone's user performed.[117] The scale, depth, and intimacy of the information police can discover during MDFT-assisted digital searches is fundamentally incomparable to any analog search method, just as the *Riley* Court warned.[118] Nor do MDFTs

---

[111] See, e.g., *Kyllo*, 533 U.S. at 36 ("[T]he technology used in the present case was relatively crude, [but] the rule we adopt must take account of more sophisticated systems that are already in use or in development") (footnote omitted).

[112] *See* Widgren, *supra* note 40, and accompanying discussion.

[113] Koepke, *supra* note 100 at 35.

[114] *Id.* at 10–30.

[115] *Id.* at 12.

[116] *Id.*

[117] *Id.* at 21–22.

[118] *Riley*, 573 U.S. at 396–97 (noting that a search of a suspect's pockets is more invasive than the most brutal home search if the suspect's pockets contain a cell phone); *see also id.* at 401 (warning that "analog[]

resemble the technologies previously contemplated by the Fourth Amendment's jurisprudence; they do not "augment[] the sensory faculties bestowed upon [officers] at birth."[119] They do more than merely help law enforcement "more efficiently conduct[]" searches.[120] They provide officers with a previously impossible analytical and invasive capability that is "otherwise unknowable."[121]

To be sure, even with a Supreme Court presence in the conversation, the reality of MDFTs indicates there is still a pressing need for additional mobile phone search requirements. With their "disturbing specter"[122] of dragnet-level search capabilities, MDFTs categorically transform mobile search warrants into potentially general searches in contravention of the Fourth Amendment's particularity requirement.[123] The most comprehensive study to date on the technology estimates that there have easily been tens of thousands of MDFT-assisted, potentially over-general searches in the last five years alone.[124] This risk is distributed nationwide: as of October 2020, "the vast majority of large U.S. law enforcement agencies have purchased or used a range of MDFTs," including the largest fifty local police departments, at least half of the fifty largest sheriff's offices, and at least sixteen of the twenty-five largest district or prosecuting attorneys' offices.[125]

MDFTs are also common among smaller law enforcement agencies, often acquired through federal grants and

---

test[s] . . . keep defendants and judges guessing for years to come") (quoting Sykes v. United States, 564 U.S. 1, 34 (2011) (Scalia, J., dissenting) (internal quotations omitted)).

[119] United States v. Houston, 813 F.3d 282, 289 (6th Cir. 2016) (quoting United States v. Knotts, 460 U.S. 276, 282 (1983)) (internal quotation marks omitted).

[120] *Id.*

[121] *Carpenter*, 138 S. Ct. at 2218; *accord Patel*, 932 F.3d at 1273.

[122] United States v. Stephens, 764 F.3d 327, 346 (4th Cir. 2014) (Thacker, J., dissenting) (discussing GPS surveillance technology), quoting United States v. Jones, 31 F.3d 1304, 1311 (4th Cir. 1994) (internal quotation marks omitted).

[123] Koepke, *supra* note 100 at 50–52.

[124] *Id.* at 41.

[125] *Id.* at 35.

inter-agency collaborations.[126] All told, at least 2,000 agencies of any size have MDFTs, and many more contract with private electronic forensic firms.[127] It is safe to say that a given mobile phone search is MDFT-assisted. The potential of being subject to one of these searches is likewise nationally distributed. Virtually every adult in the United States owns a mobile phone, the vast majority of which are smartphones.[128] These searches are usually subject to little oversight outside of *Riley* and its progeny.[129]

3. The Incomparable Disconnect Between a Phone's User Experience and Government Search

Riley, notwithstanding its enormous value, failed to identify one of the phone's most unique qualities. Unlike other technologies and their forensic investigation counterparts,[130] a

[126] *Id.* at 36–69.

[127] *Id.* at 32.

[128] 96% of U.S. adults own a cellphone and 81% of U.S. adults own a smartphone. *Mobile Phone Ownership*, PEW RESEARCH CENTER: INTERNET & TECHNOLOGY (last updated Feb. 7, 2019), http://www.pewinternet.org/chart/mobile-phone-ownership.

[129] Koepke, *supra* note 100 at 55–57. I believe it is important to note in this aside that self-governance implicates, in its own right, significant policy and legal issues. For example, while some law enforcement agencies reserve MDFTs for investigating serious crimes, many law enforcement agencies perform MDFT-assisted digital searches while investigating crimes as minor as graffiti or simple drug possession. *Id.* at 4. In fact, many criminal investigations featuring MDFT-assisted digital searches were focused on offenses with "little to no relationship to a mobile device, nor [were] the offenses digital in nature." *Id.* at 42. This is unsurprising: "[i]t 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." *Riley*, 573 U.S. at 399. Thus, the risk of over-general mobile searches created by MDFTs are mostly shouldered by persons arrested for minor crimes, who in turn were likely arrested because they were harmed by various structures and agents of whiteness, racial capitalism, and patriarchy. *See, e.g.*, Koepke, *supra* note 100 at 45, n.129. Though there is not room to address it here, I ask the reader to bear in mind that the open questions in mobile searches are, at their heart, public interest and community justice problems, institutionalized as constitutional issues.

[130] Take, for example, computers. The user of a phone and the user of a computer both use the device to store information via similar mechanisms

person stores and views information in their phone in a *significantly differently* manner—both functionally and technically—than how the government later accesses and views that information during a forensic search.

The disconnect between the user's and government's experiences is easily observed. The phone user has no meaningful control of where on the device's storage or memory the information is stored; that decision is made by the phone's manufacturers.[131] Assuming you have used a smartphone, think of how easy it is to access your SMS message conversations and your camera roll, and how little mind you pay to where in the phone's storage or memory that information lives (as compared to where on the screen you tap to retrieve it). Indeed, given how the modern smart phone prioritizes streamlined access to stored

(namely storage and memory; for a basic explanation of these mechanisms, *see Storage vs. Memory*, PC MAG (last visited Feb. 24, 2021), https://www.pcmag.com/encyclopedia/term/storage-vs-memory/). The computer user must also decide where the information is stored (*e.g.*, on an external device like a USB, on the device's hard drive, or in a particular sub-partition of either). The average computer owner also likely navigates to the information's location via file explorer (also called a file manager) or its cousin, the command line (also called a command prompt), available on all computers each time they want to access or move it (for a basic explanation of file explorers/managers, *see File Manager*, PC MAG (last visited Nov. 12, 2021) https://www.pcmag.com/encyclopedia/term/file-manager). The government forensic search of a computer heavily utilizes the same file trees and command-line features, *e.g.*, duplicating how a suspect "can mislabel or hide files and directories, . . . attempt to delete files to evade detection, or take other steps . . . . [that] may require agents and law enforcement . . . [to] peruse every file briefly to determine whether it falls within the scope of the warrant." H. Marshall Jarrett et al., Dep't of Just. Computer Crime and Intell. Prop. Sec., Crim. Div., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (3d ed. 2017). Thus there is little disconnect between the user's and government's access procedures or abilities.

[131] Android and iOS phone platforms both have a form of built-in file explorer that might afford the user some agency in this decision, but those capabilities are extremely limited in comparison to the agency an average computer's built-in file explorer affords. *See, e.g.,* Chris Hoffman, *How to Use Android 6.0's Built-in File Manager*, HOW-TO GEEK (Jul. 10, 2017, 1:22 PM), https://www.howtogeek.com/231401/how-to-use-android-6.0's-built-in-file-manager/ (noting that in Android's built-in file explorer, access to the explorer itself is hidden by design and the ability to access network storage locations or root file system is unavailable).

data, the average mobile phone owner likely does not even attempt to restructure or reorganize the phone's data once it has been created in the device. Even rarer is the mobile phone owner who attempts to retrieve or verify information they perceived was permanently deleted, making it "impractical, if not impossible," to anticipate their phone's contents being exposed to scrutiny.[132]

In stark contrast, when the government uses an MDFT to access the very same text messages and photographs, they can choose from three general methods. Through the method with the largest disconnect—closer in meaning to a chasm—the government can extract and reassemble the individual bits[133] (something that, even on the more-dexterous computer, only "superusers" can do[134]) making up the phone's storage, then pull out the bits comprising the text messages and photographs.[135] There is a less-gaping disconnect in the next option, where the government can navigate to the data via the device storage's hidden file system. Third, still distinct from (though closest to) the phone user's experience, the government can retrieve the phone's application program interface data,[136] which includes only the information that the user can access but then automatically collates and analyzes that information in a manner the user cannot replicate. In each case, without access to MDFT software themselves, the user is unable to simulate what a government search would look like; they are instead stuck navigating between apps, bereft of the option to see each piece of data laid out as a puzzle piece to their phone's bigger picture.

---

[132] United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) (emphasizing this point in terms of the high scrutiny of border searches).

[133] *See Bit*, PC MAG (last visited Feb. 24, 2021), https://www.pcmag.com/encyclopedia/term/bit/.

[134] Physical extraction involves root-level access. *See Root Level*, PC MAG (last visited Feb. 24, 2021), https://www.pcmag.com/encyclopedia/term/root-level.

[135] This option might yield, illustratively, 900 printer pages worth of information. United States v. Kolsuz, 890 F.3d 133, 136 (4th Cir. 2018), as amended (May 18, 2018).

[136] For a basic explanation of application program interfaces (APIs), *see What are APIs? - Anecdotes and Metaphors*, 18F GITHUB (last visited Feb. 24, 2021), https://18f.github.io/API-All-the-X/pages/what_are_APIs-anecdotes_and_ metaphors/ ("APIs are like the world's best retriever. You say, 'Fido - go fetch me X' and he brings you back X.")

All options, as phone searches, necessarily involve "reconstruct[ing] a considerable chunk of a person's life,"[137] and all options, being MDFT-assisted, necessarily implicate this unique disconnect.

Courts have intermittently commented on the disconnect between the mobile phone user's experience and the government's search. At the border, for instance, where the Fourth Amendment is significantly watered-down, the Fourth Circuit Court of Appeals recognized that phones implicate such significant dignitary interests that a forensic search of the defendant's phone was significantly more intrusive than a manual search would have been.[138] In the Court's words, the forensic search "might be [better] compared to a 'body cavity search' of a phone."[139]

B. *The Mobile Phone Search is Intimate and Unmatched*

1. It Clearly Invades Nearly All—if Not All—Dignitary Interests Protected by the Fourth Amendment.

A mobile phone search reconstructs "[t]he sum of an individual's private life,"[140] and implicates in the strongest sense an "individual's control of information concerning his or her person."[141] To a great extent, a phone resembles a home.[142] A person uses it to access refuge, privacy, and comfort, even when

[137] United States v. Ganias, 824 F.3d 199, 231 (2d Cir. 2016) (Chin, J., dissenting), quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) (internal quotation marks omitted).

[138] *Kolsuz*, 890 F.3d at 146 ("After *Riley* [granted protections to manual phone searches], . . . a forensic search of a digital phone must be treated as a nonroutine border search, requiring some form of individualized suspicion").

[139] *Id.* at 140 (quoting United States v. Kolsuz, 185 F.Supp.3d 843, 860 (E.D. Va. 2016).

[140] *Riley,* 573 U.S. at 396.

[141] *Patel*, 932 F.3d at 1273.

[142] *Riley*, 573 U.S. at 396-397.

they are physically in public. This is true particularly when they password-protect the device.[143]

Sensibly, people are generally more comfortable letting a friend into their house than into their phone. To a similarly great extent, a phone resembles the body in this way. A person retains a dignitary interest in the phone commensurate with their dignitary interest in bodily autonomy.[144] A person's phone is so intimate a realm as to be "an important feature of [their] human anatomy."[145] The quantity and quality of information a person stores in their phone, ranging from their medical, to political, to social lives,[146] indicates that for many, a stranger (let alone the government) thumbing through their device and analyzing its contents[147] would be a "harmful, humiliating, and degrading" experience.[148] "The fact that technology now allows an individual to carry [that] information in his hand does not make the information any less worthy of the protection for which the Founders fought."[149]

2. It Falls Between Searches of the Home and the Body on the Continuum.

Consider the mobile phone in terms of the factors affecting continuum placement.[150] The *Riley* Court has saved us some time here. The Court decided not to exempt mobile phone searches from the warrant requirement.[151] The mobile phone

---

[143] Aaron Smith, *Password management and mobile security*, PEW RESEARCH CENTER: INTERNET & TECHNOLOGY (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security/.

[144] *Kolsuz*, 890 F.3d.

[145] *Riley*, 573 U.S. at 391.

[146] *See supra* notes 90–91. *See also id.*, 573 U.S. at 396 (noting that phones implicate "a wealth of detail about her familial, political, professional, religious, and sexual associations"), quoting *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (internal quotation marks omitted).

[147] *Carpenter*, 138 S. Ct. at 2218.

[148] *Florence*, 566 U.S. at 345.

[149] *Riley*, 573 U.S. at 403.

[150] *See generally supra*, I.C. THE SEARCH'S PLACEMENT ON THE CONTINUUM IS A FUNCTION OF ITS EXTENT AND NATURE, ADJUSTING FOR RELEVANT FACTS; EXAMPLES.

[151] *Riley*, 573 U.S. at 403.

search is then at least further right on the continuum than the warrant threshold. The Court also determined that the phone is afforded at least the "degree of privacy against government that existed when the Fourth Amendment was adopted,"[152] even more so than the home is.[153] The mobile phone search moves further to the right, past the search of the home, as it more substantially endangers the subject's dignitary interests. However, the phone is at most a "feature" of the human body,[154] and certainly not so physically and fundamentally related to our persons as to give us "instinctively . . . the most pause."[155] Thus, the mobile phone search is not as far right as searches of the body. But perhaps it is close, especially when the search is forensic.[156]

So there is a well-defined segment of the continuum which mobile phone searches lay on: between searches of the home and the body. The *Riley* Court (deliberately[157]) did not address the last significant factor that would help clarify placement further: adjacent doctrines of Fourth Amendment law. But those doctrines are justified by the balance of law enforcement and privacy interests,[158] something that Justices Alito and Sotomayor suggest may be restruck based on the nature of mobile phones[159] and the digital age,[160] respectively.

---

[152] *Jones*, 565 U.S. at 406.

[153] *Riley*, 573 U.S. at 393.

[154] *Id.* at 395.

[155] *Wolfish*, 441 U.S. at 558 (concerning body cavity searches).

[156] *See Kolsuz*, F.Supp.3d at 860.

[157] *Riley*, 573 U.S. at 395, n.1 ("[T]hese cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

[158] *Riley*, 573 U.S. at 385 (quoting *Houghton*, 526 U.S. at 300 (internal quotation marks omitted)).

[159] *Riley*, 573 U.S. at 406–07 (Alito, J., concurring) ("[W]e should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. *This calls for a new balancing* of law enforcement and privacy interests") (emphasis added).

[160] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("*[I]t may be necessary to reconsider* the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great

That balance has already been shown to hang in a meaningfully different way as far as historic cell phone location information is concerned.[161] Similarly, in comparison to other searches, a phone's contents give law enforcement access to information about the subject that is "otherwise unknowable."[162]

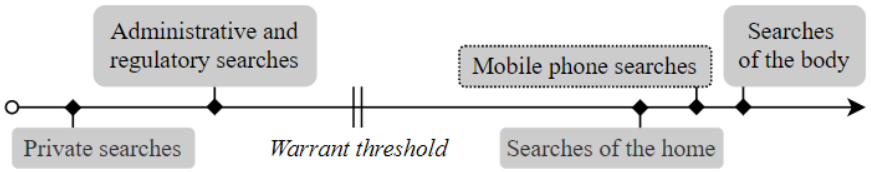

FIGURE 3. The mobile phone search on the continuum.

III. MOBILE PHONE SEARCHES MERIT *SUI GENERIS* FOURTH AMENDMENT TREATMENT

In Part III I take a brief excursion into what it means for a thing to be *sui generis* in the law's eyes. Then I set out four reasons, building on the arguments I set out in Parts I and II, to advocate for mobile phone searches to be designated *sui generis* in the Fourth Amendment.

A. *What it Means to be* Sui Generis

Sui generis, a legal term of art,[163] is without clear instructions. "Legal principles must treat instances alike. Those principles do not permit treating" certain situations separately from others "without a satisfying explanation of why" those situations are separate (*sui generis*).[164] For example, the Supreme Court was unsatisfied with the mere fact of wartime as

deal of information about themselves to third parties in the course of carrying out mundane tasks") (internal citations omitted) (emphasis added).

[161] *Carpenter*, 138 S. Ct. at 2220 (holding the third-party doctrine does not reach historic cell site location information because such information "implicates privacy concerns far beyond those considered" in the doctrine's seminal cases).

[162] *Id.* at 2218.

[163] "Of its own kind or class; unique or peculiar." *Sui Generis*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[164] Morse v. Frederick, 551 U.S. 393, 426–27 (2007).

justification to mandate the Pledge of Allegiance during World War II as *sui generis* to First Amendment speech.

Sui generis designation signals that the substance of a situation is inherently unique and cannot be evaluated "by automatic reference to the law of ordinary" instances; it "must be governed by unique, separate, and distinct rules."[165] Designation is often used to limit the application of a rule—leaving more conduct less regulated—but it can be designated to require heightened standards as well.[166] In the context of the Fourth Amendment, examples may be illuminating:

a. A *Terry* frisk (also known as a stop-and-frisk) is a *sui generis* search because it is "brief" and "minimal[ly] intrusi[ve]."[167]

b. A canine sniff by a well-trained narcotics-detection dog is a *sui generis* search because it "discloses only the presence or absence of narcotics, a contraband item."[168]

c. Any search at the border is a *sui generis* search, given the broad constitutional power the federal government has at the border, merely "by virtue of the person's or thing's entry into [the United States] from the outside."[169]

d. Any search of a person on probation or parole is a *sui generis* search because, simply by being in such a program, the person's dignitary interests are mitigated

[165] United States v. Hill, 967 F.2d 902, 910 (3d Cir. 1992) (citing Latta v. Fitzharris, 521 F.2d 246, 251 (9th Cir.), *cert. denied*, 423 U.S. 897 (1975)).

[166] The most well-known example is perhaps radio broadcasting and the First Amendment. *See* Fed, Commc'ns Comm'n v. Pacifica Foundation, 438 U.S. 726 (1978).

[167] United States v. Guzman-Padilla, 573 F.3d 865, 883–84 (9th Cir. 2009) (quoting Dunaway v. New York, 442 U.S. 200, 209–10 (1979)).

[168] Illinois v. Caballes, 543 U.S. 405, 409 (2005) (citing *Place*, 462 U.S. 696, 707 (1983)).

[169] United States v. Sanders, 663 F.2d 1, 2–3 (2d Cir. 1981) (citing United States v. Ramsey, 431 U.S. 606, 619 (1977)).

and the government's interest in preventing future community harm is heightened.[170]

B. Sui Generis *Dignitary Interests Merit* Sui Generis *Treatment*

Mobile phone searches implicate *sui generis* dignitary interests, meriting *sui generis* Fourth Amendment treatment. Four distinct reasons buttress this argument.

First, the phone search's placement on the continuum between searches of the sacrosanct home and sacrosanct body signals that it is sacrosanct itself, more deserving of "unique, separate, and distinct rules"[171] than the less-sacred searches further to its left on the continuum.

Second, a person sees information in their phone incomparably differently than how the government sees that information during a forensic search of it. This disconnection uniquely prevents a person from exercising meaningful control over their information or dignitary interests.[172] Like the *sui generis* narcotics-detection dog sniff,[173] the MDFT is unique among investigative procedures in terms of the manner and type of information it is used to reveal. To be sure, the disconnect and comparison is weaker if the search is unaided by an MDFT. But—without commenting on the merits of their justifications—the government will not always be completely transparent about their MDFT use.[174] And, without commenting on the merits of the practice, the government will generally have access to MDFTs in a given phone search.[175] Every phone embodies the same minimum (and significant) dignitary interests; if *sui*

[170] *See, e.g.*, Griffin v. Wisconsin, 483 U.S. 868, 874–75 (1987) (finding search of person on probation *sui generis*); *Hill*, 967 F.2d at 910 (finding search of person on parole sui generis); *accord Latta*, 521 F.2d at 250–51 (finding search of person on parole *sui generis*).

[171] *Hill*, 967 F.2d at 910.

[172] *See Patel*, *supra* note 33.

[173] *See Caballes*, 543 U.S. at 409.

[174] Koepke, *supra* note 100 at 70–71 (discussing proof of MDFT use by law enforcement agencies that otherwise denied public records requests).

[175] *Id.* at 32.

generis designation was limited to MDFT-assisted searches, police departments not openly possessing an MDFT[176] would get a windfall compared to those known to use MDFTs. Worse yet, police departments would be incentivized to conceal any positive MDFT capabilities they possess. There is no compelling policy reason to allow either consequence so courts must address all cases as if MDFTs were used.[177]

Third, as a policy matter, *sui generis* designation acknowledges that every major milestone in Fourth Amendment jurisprudence has empowered individuals to act deliberately regarding the security of their personal affairs.[178] Now that personal affairs are stored on mobile phones—not to mention every quantitative and qualitative difference the *Riley* Court makes between phones and their historical analogs[179]—a new major milestone such as the designation would be appropriate (and to some, possibly overdue[180]).

Fourth, *sui generis* designation furthers Fourth Amendment jurisprudence in the context of mobile phones and new technologies generally. It provides the government with a "workable rule[] . . . done on a categorical basis"[181] in conducting phone searches and gives courts the ability to reconsider traditional Fourth Amendment doctrines in mobile phone searches with fewer obstacles.[182]

---

[176] Meaning there are public records indicating they possess or regularly use an MDFT, like those documented by Koepke et al., *id*.

[177] *See Riley*, 573 U.S. at 403 (noting workable rules "must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers" or agencies), quoting Michigan v. Summers, 452 U.S. 692, 705, n.19 (1981) (internal quotation marks omitted).

[178] Most famously *Katz*, 389 U.S., and the "third-party" doctrinal cases, *e.g.*, *Smith*, 442 U.S., and *Miller*, 425 U.S.

[179] *See Riley*, 573 U.S.

[180] *See supra* notes 159–160.

[181] *Riley*, 573 U.S. at 398, quoting *Summers*, 452 U.S. at 705, n.19 (internal quotation marks omitted).

[182] Courts may also more easily build on the work done thus far. On the plain view doctrine, *see, e.g.*, Kerr and Ohm, *supra* note 106, Koepke, *supra* note 100. On the third-party doctrine, *see, e.g.*, Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (identifying a limit on the third-party doctrine and holding that a "home

This is particularly attractive. In resolving those complexities, the Fourth Amendment, familiarly known as a mosaic (and, less endearingly, as a mess) "maintains the integrity" of its existing legal rules[183] and "furthers rather than undermines the doctrinal consistency of . . . [the related] jurisprudence."[184] To that end, in developing the phone search's constitutional canon, courts will fashion for themselves a blueprint for answering questions presented by future technological innovations. That design will necessarily correspond with my posited continuum, measuring the technology's Fourth Amendment implications in terms of the interests it comprises, instead of the "esoteric"[185] method its search entails.[186] The designation helps answer "the difficult

occupant does not assume the risk of near constant monitoring [by a smart utility meter] by choosing to have electricity in her home"), citing *Carpenter*, 138 S. Ct. at 2220. On the question of general warrants, *see, e.g.*, *supra* notes 100–106, discussion in *Ganias*, 824 F.3d at 233 (Chin, J., dissenting) ("[b]y barring the Government from simply taking *everything* through the use of a general warrant, the Fourth Amendment contemplates that investigators may miss *something*. With computers, another search term can always be concocted and data can always be further crunched. But the fact that another iota of evidence might be uncovered at some point down the road does not defeat the rights protected by the Fourth Amendment"). And on the question of super-warrants: if courts determine the phone search is close enough to the body search as to require "clear indication" a search would be fruitful, *Schmerber*, 384 U.S. at 770, should it be similarly harder to acquire a warrant for a phone search? It would be the "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." *Riley*, 573 U.S. at 399.

[183] Charles J. Keeley III, *Subway Searches: Which Exception to the Warrant and Probable Cause Requirements Applies to Suspicionless Searches of Mass Transit Passengers to Prevent Terrorism?*, 74 FORDHAM L. REV. 3231, 3288 (2006).

[184] *Id.* (citing Michigan Law Review, *The Constitutionality of Airport Searches*, 72 MICH. L. REV. 128, 153 (1973) (internal quotation marks omitted)).

[185] *Smith*, 442 U.S. at 749, n.1 (Marshall, J., dissenting).

[186] *Riley*, 573 U.S. at 407 (Alito, J., concurring) (Courts could develop nuanced rules for new technologies, but "during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change").

legal issues raised by new technology" and primes them to "be[] addressed."[187]

I close by noting that *sui generis* designation here would not come at the cost of other *sui generis* case law. It is likely, for instance, that courts will find allowing the *sui generis* border search furthers a more compelling interest than preventing the *sui generis* phone search.[188] It would also not be out of line with current practice for a court to find that the *sui generis* search of a person on probation is less worthy than the *sui generis* phone search.[189] In any case, *sui generis* searches have interacted with each other before and, as all Fourth Amendment searches must respect the same fundamental dignitary interests, courts are well-equipped to address those questions as they arise.

IV. CONCLUSION

A hidden pattern in Fourth Amendment jurisprudence—a continuum of protections that shield a person's dignitary interests from government invasion—helps students, scholars, and jurists alike analyze what protections the Fourth

[187] This is in contrast to the standard criticism of over-nuancing the Fourth Amendment jurisprudence as an answer to technological innovation. Attkisson v. Holder, 925 F.3d 606, 643 (4th Cir. 2019), as amended (June 10, 2019) (Wynn, J., concurring in part) (disagreeing with the majority insofar as they "avoid[] the difficult legal issues raised by new technology by erecting procedural barriers that ensure they never will be addressed").

[188] *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (holding that laptops and personal electronic devices can be searched without reasonable suspicion at the border); *see also* United States v. Touset, 890 F.3d 1227, 1234 (11th Cir. 2018) (refusing to rely on *Riley* at all and finding that reasonable suspicion is not required to search a phone), Alasaad v. Mayorkas, No. 20-1077, 2021 WL 521570, at *6 (1st Cir. Feb. 9, 2021) (holding the same as *Touset*, stating that "privacy concerns, however significant or novel, are nevertheless tempered by the fact that the searches are taking place at the border"). *But see Kolsuz*, 890 F.3d at 144 (requiring "individualized suspicion" to search a phone using forensic technology).

[189] *See, e.g.*, United States v. Fletcher, 978 F.3d 1009, 1019 (6th Cir. 2020), *reh'g denied* (Dec. 14, 2020) (declining to find that defendant, in consenting to probation agreement authorizing the search of his person or place of residence, also authorized search of his mobile phone). *But see* United States v. Johnson, 875 F.3d 1265, 1274 (9th Cir. 2017) (finding that the privacy interest of defendant on parole was diminished enough to make a warrantless search of their cell phone constitutional).

Amendment affords a person against a given search. Without mechanically applying any rules or factors, it clearly illustrates searches' comparative invasiveness, honoring the *Katz* and trespassory tests and their progeny at the heart of the Fourth Amendment.

This continuum proves especially valuable in analyzing the protections afforded against technology-involved searches, particularly the technology most intimately connected to the greater population: mobile phones. This analysis is pressing. Not only are phones, and searches thereof, more frequent every day, but the asymmetry between the person's use of their phone and the government's search of it is unmatched among personal technologies. Applying the continuum framework makes it apparent that mobile phone searches land between searches of the home and body in sacredness and, therefore, in dignitary interests. This placement, in tandem with the incomparable disconnect of search methods, the policy reasons favoring another milestone in Fourth Amendment case law, and the blueprint it would create for future technologies, merits the mobile phone search being designated *sui generis* for Fourth Amendment purposes.