IDENTIFYING FOURTH AMENDMENT VALUES: AN EVIDENCE-BASED APPROACH

Christopher S. Yoo[*] *& Arnav Jagasia*[**]

Scholars have widely criticized the Supreme Court's Fourth Amendment jurisprudence as incoherent, especially in cases involving emerging technologies. This Article argues that to understand Fourth Amendment doctrine, one must consider how the values that underlie the Court's decisions are balanced against each other and shift over time. To do so, this Article first proposes a novel, bottom-up approach to identifying the relevant values that focuses on the specific evidence that the Court considers in each case. Distilling the values underlying the Fourth Amendment provides a more coherent understanding of Fourth Amendment doctrine. This Article then applies this framework to three biometric technologies: facial recognition, iris recognition, and DNA profiling. Law enforcement use of these technologies may all raise Fourth Amendment challenges, but the framework shows how these challenges implicate different values. Recognition and application of this framework can result in a better appreciation of the impact of emerging technologies on Fourth Amendment doctrine.

TABLE OF CONTENTS

INTRODUCTION 1221
I. EVIDENCE AS THE BASIS FOR FOUR PERSPECTIVES ON THE FOURTH AMENDMENT 1225
  A. *The Law Enforcement Conduct Factor (Factor 1)/Prevention of Governmental Abuse* 1225

* Imasogie Professor in Law and Technology, Professor of Communication, Professor of Computer and Information Science, Founding Director of the Center for Technology, Innovation & Competition, University of Pennsylvania.

** Head of Software Engineering for Privacy and Responsible AI, Palantir Technologies. The authors would like to thank Stephanos Bibas, Orin Kerr, Matthew Tokson, Rebecca Wexler, and participants in presentations at the Privacy Law Scholars Conference and the University of Pennsylvania Carey Law School for their comments on previous versions of this Article. The views expressed in this Article are solely those of the authors.

1. The Location from Which the Surveillance Was Conducted (Factor 1A) 1226
2. The Enablement of Indiscriminate, Dragnet Searches (Factor 1B) 1229
B. The Defendant Conduct Factor (Factor 2)/Fairness to the Defendant 1230
1. Exposure by the Defendant (Factor 2A) 1230
2. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B) 1235
a. Technology and Knowledge 1235
b. Technology and Voluntariness 1237
C. The Information Sensitivity Factor (Factor 3)/Protection of the Substantive Privacy Interests of the Defendant 1238
1. The Sensitivity of the Home 1238
2. The Sensitivity of Location Information 1241
3. Direct Analysis of Information Sensitivity 1242
D. The Societal Impact Factor (Factor 4)/Aggregate Social Welfare 1244
1. The Social Benefits of More Effective Law Enforcement (Factor 4A) 1244
2. The Social Costs of Avoidance Behavior (Factor 4B) 1247
E. The Underlying Values and the Relative Importance of the Factors 1249
II. EMERGING BIOMETRIC TECHNOLOGIES 1251
A. Facial Recognition Technology (FRT) 1252
1. The Law Enforcement Conduct Factor (Factor 1) 1254
2. The Defendant Conduct Factor (Factor 2) 1255
a. Exposure by the Defendant 1255
b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant 1256
3. The Information Sensitivity Factor (Factor 3) 1258
4. The Societal Impact Factor (Factor 4) 1259
a. The Social Benefits of More Effective Law Enforcement (Factor 4A) 1260
b. The Social Costs of Avoidance Behavior (Factor 4B) 1261
5. Summation 1262
B. Iris Recognition Technology 1262
1. The Law Enforcement Conduct Factor (Factor 1) 1264
2. The Defendant Conduct Factor (Factor 2) 1264
a. Exposure by the Defendant (Factor 2A) 1264
b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B) 1265
3. The Information Sensitivity Factor (Factor 3) 1267
4. The Societal Impact Factor (Factor 4) 1268

a. The Social Benefits of More Effective Law Enforcement (Factor 4A).....1268
b. The Social Costs of Avoidance Behavior (Factor 4B).....1268
5. Summation.....1269
C. DNA Profiling.....1269
1. The Law Enforcement Conduct Factor (Factor 1)...1272
2. The Defendant Conduct Factor (Factor 2).....1275
a. Exposure by the Defendant (Factor 2A).....1275
b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B).....1276
3. The Information Sensitivity Factor (Factor 3).....1277
4. The Societal Impact Factor (Factor 4).....1278
a. The Social Benefits of More Effective Law Enforcement (Factor 4A).....1278
b. The Social Costs of Avoidance Behavior (Factor 4B).....1279
5. Summation.....1279
III. SYNTHESIS OF FRAMEWORK.....1280

INTRODUCTION

Two insights have long informed the analysis of the Fourth Amendment. First, scholars have uniformly criticized the Supreme Court's Fourth Amendment jurisprudence as incoherent[1] despite their best efforts to advance a unifying theory synthesizing the doctrine.[2] Second, the Court has exhibited significant ambivalence

1. *See* Carpenter v. United States, 138 S. Ct. 2206, 2244 & n.10 (2018) (Thomas, J., dissenting) (citing a wide array of scholarly and judicial criticism of Fourth Amendment doctrine); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505 (2007) (noting that "[a]mong scholars," the state of Fourth Amendment doctrine "is widely considered an embarrassment" and that "[t]he Court's handiwork has been condemned as 'distressingly unmanageable,' 'unstable,' and 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended'" (alteration in original) (footnotes omitted)); Nicholas Kahn-Fogel, *An Examination of the Coherence of Fourth Amendment Jurisprudence*, 26 CORNELL J.L. & PUB. POL'Y 275, 278 (2016) (observing that "authors have characterized the Court's pronouncements on the Fourth Amendment as 'illogical, inconsistent with prior holdings, and, generally, hopelessly confusing'; 'a mass of contradictions and obscurities'; 'an embarrassment'; 'arbitrary, unpredictable, and often border[ing] on incoherent'; 'lack[ing] a coherent explanation'; and 'subjective, unpredictable, and conceptually confused'" (footnotes omitted)).

2. *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011) (calling the Fourth Amendment "a theoretical embarrassment to scholars and judges alike"). For a general

toward technological change, sometimes welcoming its benefits,[3] sometimes warning about its potential to encroach upon privacy,[4] and at still other times adopting a more tentative, wait-and-see attitude.[5]

Undeterred by the failure of past efforts, we offer another attempt to make sense of the Fourth Amendment that employs a different methodology. Attempts to unify Fourth Amendment doctrine typically follow a top-down approach through the application of proffered first principles.[6] Such analyses struggle to explain the variation in the Court's Fourth Amendment decisions, making the Court's decisions over time on seemingly similar cases hard to reconcile into a unified, timeless understanding of the Fourth Amendment.[7]

We contend that the truest indicator of the values underlying the Fourth Amendment is the evidence on which the Court focused when making its decision. Adopting this evidence-based lens, we find that the Supreme Court's Fourth Amendment decisions focus on four different types of evidence designed to illuminate four distinct values:

---

critique of Fourth Amendment theory, see Ronald J. Alen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1161–89 (1998) (critiquing scholarly attempts to advance a unifying a theory of the Fourth Amendment).

3. *See* United States v. Knotts, 460 U.S. 276, 282 (1983) (arguing that the Fourth Amendment does not prohibit "the police from augmenting their sensory faculties with such enhancement as science and technology afforded them in this case"); Maryland v. King, 569 U.S. 435, 459 (2013) (acknowledging DNA as a technology so superior to fingerprinting in identifying individuals that "to insist on fingerprints as the norm would make little sense to either the forensic expert or a layperson").

4. *See Carpenter*, 138 S. Ct. at 2214 (acknowledging the need to protect privacy against technology's ability to "encroach upon areas normally guarded from inquisitive eyes"); Kyllo v. United States, 533 U.S. 27, 34 (2001) (acknowledging technology's ability "to erode the privacy guaranteed by the Fourth Amendment").

5. *See* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *Knotts*, 460 U.S. at 284 (reserving judgment on "dragnet-type law enforcement practices" that might raise more serious Fourth Amendment concerns).

6. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994); *see also* Kerr, *supra* note 1, at 550 ("The Justices simply cannot embrace a top-down approach regardless of how protective it may be. Instead of offering new top-down models, scholars should recognize that the principles guiding what is a 'search' must necessarily be decentralized.").

7. *See* Kerr, *supra* note 2, at 479–80 (outlining seemingly incoherent Fourth Amendment decisions in Supreme Court cases with similar facts); Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 4 UTAH L. REV. 977, 978 (2004) (explaining that the Court chooses among many models to analyze "reasonableness," which leads to changing views on what constitutes a search).

(1) The conduct of law enforcement, which reflects the prevention of abuse by governmental officials;
(2) The conduct of the defendant, which reflects fairness to the defendant;
(3) The sensitivity of the information gathered, which reflects the defendant's substantive privacy interests; and
(4) The impact of the surveillance on society, which reflects the promotion of social welfare.

These different evidentiary factors reflect different values relevant to the Fourth Amendment. Examining the conduct of law enforcement views the Fourth Amendment as a negative limit on the government and frames surveillance as a potential form of authoritarian abuse. Focusing on the conduct of the defendant emphasizes relational norms that are particular to individuals, specifically with respect to fairness. Concentrating on the sensitivity of the information gathered reflects the defendant's positive privacy rights as a substantive matter. Looking at impact on society takes into account the impact that permitting or forbidding the surveillance in question would have on others and society as a whole. In short, the types of evidence that the Court has considered provides a powerful lens for surfacing and categorizing the values underlying any particular Fourth Amendment decision. A better understanding of those values and how they have changed over time can serve as the basis for a more coherent understanding of Fourth Amendment doctrine.

Technological change provides a natural source of variation needed to determine the impact of different values that influence the Court's Fourth Amendment decisions. Improvements in technology provide law enforcement with new methods to investigate suspects, leading to new unregulated methods for searches that inevitably raise Fourth Amendment concerns. It is no accident that changes in technology—electronic eavesdropping,[8] tracking devices,[9] aerial surveillance,[10] thermal imaging scanners,[11] and cell phones[12]—have provided the loci for the most important Fourth Amendment decisions over the past few decades. Analyzing the Court's treatment of evidence in these cases of technological change reveals why certain

8. Smith v. Maryland, 442 U.S. 735, 736 & n.1 (1979); Katz v. United States, 389 U.S. 347, 349–50 (1967).

9. United States v. Jones, 565 U.S. 400, 402 (2012); United States v. Karo, 468 U.S. 705, 707 (1984); *Knotts*, 460 U.S. at 277.

10. Florida v. Riley, 488 U.S. 445, 447–48 (1989); California v. Ciraolo, 476 U.S. 207, 213–14 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

11. Kyllo v. United States, 533 U.S. 27, 29 (2001).

12. Carpenter v. United States, 138 S. Ct. 2206 (2018); Riley v. California, 573 U.S. 373, 403 (2014).

types of evidence raise Fourth Amendment concerns—or are dismissed as unproblematic.

In this Article, we focus our analysis on the Court's Fourth Amendment decisions in cases of technological change. Part I develops the four evidentiary factors that the Court considers when applying the Fourth Amendment to a case. Part II applies this framework to three emerging biometric technologies—facial recognition, iris recognition, and DNA profiling—that raise Fourth Amendment challenges. Part III synthesizes the application of the framework and reveals how the different evidentiary factors can motivate the Court's decision about a search toward or away from reasonableness.

We believe this Article sets forth a comprehensive schema of Fourth Amendment values identified through a novel, evidence-based approach. In advancing this argument, we do not pretend to be the first to have examined the impact of the individual components we discuss.[13] That said, our analysis develops each component in novel ways, and to our knowledge, no previous scholars have integrated them into the framework we lay out here.

The insights of Hume's guillotine also make clear that any inherently descriptive analysis, such as ours, necessarily cannot establish its normative merits. We do not argue for a normative weighing of these factors. In fact, the relative importance of each factor may change over time and is influenced by social and technological context. That said, analyzing the positive reality can serve as an important step in reaching a reflective equilibrium. It can also reveal the extent to which some analyses focus on one aspect to the exclusion of others or muddle the analysis by unconsciously shifting among different rationales without acknowledging it. In addition, analyzing the prevalence of these factors across different cases can reveal how their importance to the Court has changed over time. Indeed, we identify a broader shift from ascriptive approaches to the Fourth Amendment in favor of a vision that focuses on the reality of privacy in practice.

---

13. For an example of a classic argument that the focus of the Fourth Amendment is misconduct by law enforcement officers, see TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION: SEARCH, SEIZURE, AND SURVEILLANCE AND FAIR TRIAL AND FREE PRESS 23–44 (1969). For an example of a prior analysis focusing on the conduct of the defendant, see Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 564–66, 569–75 (1990). For an example of a discussion focusing on the sensitivity of the information, see Kerr, *supra* note 1, at 512–15. For an example of a discussion of the effectiveness of law enforcement, see Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 366–69 (2019).

I. EVIDENCE AS THE BASIS FOR FOUR PERSPECTIVES ON THE FOURTH AMENDMENT

In this Part, we lay out the four types of evidence to which the Supreme Court has looked when applying the Fourth Amendment to a particular case. Each, in turn, implicates distinct Fourth Amendment values. We also note, as a preliminary matter, that the Fourth Amendment requires two separate inquiries: first, whether a search has occurred, and second, if so, whether the search was reasonable.[14] The first three factors we identify focus on the first inquiry, while the fourth factor focuses on the second.

A. The Law Enforcement Conduct Factor (Factor 1)/Prevention of Governmental Abuse

The Supreme Court has long placed the actions of law enforcement at the center of its Fourth Amendment jurisprudence.[15] As the Supreme Court recognized in its seminal Fourth Amendment decision in *Boyd v. United States*,[16] the need to protect citizens from indiscriminate intrusions by government officials, enabled by general warrants and writs of assistance that characterized the colonial era, galvanized not only the Fourth Amendment but also the entire Revolutionary movement.[17] Moreover, defining the Fourth

---

14. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2215 n.2 (distinguishing between "the threshold question whether a 'search' has occurred" and "the separate matter of whether the search was reasonable"); *Kyllo*, 533 U.S. at 31 (similarly distinguishing between "the antecedent question whether or not a Fourth Amendment 'search' has occurred" from "whether a . . . search . . . is reasonable").

15. *See* Ohm, *supra* note 13, at 372 (noting that "most Fourth Amendment analyses of the past . . . almost always placed police action and individual counter-action at the center").

16. 116 U.S. 616 (1886).

17. *Id.* at 624–30. As the Court eloquently stated in *Stanford v. Texas*:

> Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists. The hated writs of assistance had given customs officials blanket authority to search where they pleased for goods imported in violation of British tax laws. They were denounced by James Otis as "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," because they placed "the liberty of every man in the hands of every petty officer." The historic occasion of that denunciation, in 1761 at Boston, has been characterized as "perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country. 'Then and there,' said John Adams, 'then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'"

Amendment in negative terms as a limit on government is consistent with the Weberian concerns about the state's monopoly on the legitimate use of physical force.[18]

For most types of investigatory practices, the Court examines the details of the conduct of law enforcement to ensure that it did not exceed permissible bounds, often focusing on the location where the surveillance was conducted. In some instances, the Court has also looked beyond the specifics of the particular case and analyzed the impact of a practice as a general matter by exploring whether the practice could constitute the type of dragnet search authorized by general warrants and writs of assistance.

1. The Location from Which the Surveillance Was Conducted (Factor 1A)

Many cases assess the propriety of law enforcement officials' conduct by asking whether they gathered information from a location where they were permitted to be. Historically, this inquiry was a matter of positive law. For example, the Court has long recognized that law enforcement officials may seize any evidence in plain view from a location where they are authorized to be, such as when arresting the defendant.[19] One traditional measure of the propriety of the officials' location turned on whether they were committing common law trespass.[20] This rationale is developed most completely in the Court's early precedents on electronic eavesdropping, which upheld the admissibility of evidence when its collection did not require a physical trespass[21] but blocked it when it required "a

379 U.S. 476, 481–82 (1965) (quoting *Boyd*, 116 U.S. at 625). For an example of modern reaffirmations of this insight, see *Carpenter*, 138 S. Ct. at 2213; *Byrd v. United States*, 138 S. Ct. 1518, 1526 (2018); and *Riley v. California*, 573 U.S. 373, 403 (2014).

18. Max Weber, *Politics as a Vocation*, *in* FROM MAX WEBER: ESSAYS IN SOCIOLOGY 77, 78 (H.H. Gerth & C. Wright Mills eds. & trans., 1946) (1919).

19. *See* Marron v. United States, 275 U.S. 192, 199 (1927).

20. *Carpenter*, 138 S. Ct. at 2213 ("For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' . . . ."); *accord* United States v. Jones, 565 U.S. 400, 405 (2012) (observing that "our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century"); Kyllo v. United States, 533 U.S. 27, 31 (2001) (similarly noting that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass").

21. *See* Olmstead v. United States, 277 U.S. 438, 456–57 (1928) (emphasizing that the wiretaps in question "were made without trespass upon any property of the defendants"); Goldman v. United States, 316 U.S. 129, 134–35 (1942) (upholding the admission of evidence collected by a listening device placed against the wall of an adjacent office was not materially aided by any trespass); On Lee v. United States, 343 U.S. 747, 749–53 (1952) (upholding the admissibility of evidence collected via a microphone and transmitter worn by a confidential informant when "no trespass was committed").

physical invasion of the petitioner's premises."[22] Yet the Court's "open fields" doctrine belied the centrality of trespass by upholding the seizure of evidence in plain view outside the house even if officials had to commit trespass to see it.[23]

As the Court has noted,[24] the Court deviated from its property-based approach in *Katz v. United States*[25] when it "departed from the narrow view"[26] that "surveillance without any trespass . . . fell outside the ambit of the Constitution"[27] and famously declared that "the Fourth Amendment protects people, not places."[28]

At the same time, the *Katz* Court adhered to the principle that the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public, *even in his own home or office*,"[29] a concept that the Court reaffirmed in *Oliver v. United States*,[30] in which it held that *Katz* did not overturn the open fields doctrine.[31]

The precise role of trespass has been a bone of contention ever since. Although some decisions attempted to decouple trespass and the Fourth Amendment completely by declaring that "an actual trespass is neither necessary nor sufficient to establish a constitutional violation,"[32] property concepts remained influential in determining the propriety of actions of law enforcement officials. For example, the Court's aerial surveillance decisions placed great weight on whether the evidence was collected from a location where the public was legally entitled to be,[33] although that view did not

---

22. Silverman v. United States, 365 U.S. 505, 510 (1961).

23. Hester v. United States, 265 U.S. 57, 59 (1924).

24. *See Kyllo*, 533 U.S. at 48–49.

25. 389 U.S. 347 (1967).

26. *Id.* at 351.

27. *Id.*

28. *Id.* at 353. For prior cases offering a similar observation, see *Warden v. Hayden*, 387 U.S. 294, 304 (1967) (recognizing that "[t]he premise that property interests control the right of the Government to search and seize has been discredited"); and *Silverman v. United States*, 365 U.S. 505, 511 (1961) (holding that the Fourth Amendment was not tied to "ancient niceties of tort or real property law"). For more recent restatements, see *Kyllo v. United States*, 533 U.S. 27, 32 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property . . . ."); and *Soldal v. Cook County*, 506 U.S. 56, 64 (1992) ("*Katz* . . . effectively ended any lingering notions that the protection of privacy depended on trespass into a protected area.").

29. *Katz*, 389 U.S. at 351 (emphasis added).

30. 466 U.S. 170 (1984).

31. *See id.* at 177.

32. United States v. Karo, 468 U.S. 705, 713 (1984).

33. *See* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (upholding the admissibility of evidence collected "from a public vantage point where [the law enforcement official] has a right to be" and that the Fourth Amendment has never "require[d] law enforcement officers to shield their eyes when passing by a home

command a majority in the Court's most recent decision in this line of precedent.[34] Later, in *Soldal v. Cook County*,[35] the Court continued to assert that trespass was sufficient by itself to establish a Fourth Amendment violation.[36]

The Court provided its strongest reaffirmation of the sufficiency of trespass in *United States v. Jones*,[37] which held that placing a tracking device on the defendant's vehicle was sufficient without more to constitute a violation of the Fourth Amendment.[38] According to the Court, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test," and neither *Katz* nor trespass constituted the exclusive test of a Fourth Amendment violation.[39] Justice Sotomayor provided the critical fifth vote for this decision, authoring a separate concurrence emphasizing that, while trespass is sufficient, it is not necessary to establish a Fourth Amendment violation and to reserve judgment on the constitutionality of the types of nontrespassory means of surveillance raised by Justice Alito.[40] The Court reiterated this principle in *Florida v. Jardines*,[41] which it supplemented with the practical observation that "[o]ne virtue of the Fourth Amendment's property-rights baseline is that it keeps easy cases easy."[42]

Other opinions have questioned whether proof of trespass is sufficient. As Justice Alito noted on behalf of four Justices in *Jones*, such an argument is hard to square with the Court's open fields doctrine.[43] Moreover, the majority opinion in *Carpenter v. United States*[44] raises similar questions. On the one hand, the Court gave some room for property rights when it observed that "no single rubric definitively resolves which expectations of privacy are entitled to

---

on public thoroughfares" or from conducting "simple visual observations from a public place"); United States v. Knotts, 460 U.S. 276, 282 (1983) (acknowledging that law enforcement may conduct "[v]isual surveillance from public places" without violating the Fourth Amendment).

34. *Compare* Florida v. Riley, 488 U.S. 445, 449–52, 452 n.3 (1989) (plurality opinion) (concluding evidence was admissible because it was gathered from legally navigable airspace), *with id.* at 453–54 (O'Connor, J., concurring in the judgment) (rejecting legality as the touchstone of constitutionality).

35. 506 U.S. 56 (1992).

36. *Id.* at 64 (holding that *Katz* did not "snuff[] out the previously recognized protection for property").

37. 565 U.S. 400 (2012).

38. *Id.* at 404–05, 406 n.3.

39. *Id.* at 409, 411.

40. *Id.* at 414 (Sotomayor, J., concurring).

41. 569 U.S. 1 (2013).

42. *Id.* at 11.

43. United States v. Jones, 565 U.S. 400, 420–21 (2012) (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

44. 138 S. Ct. 2206 (2018).

protection" and that "property rights are often informative."[45] On the other hand, the *Carpenter* majority concluded that *Katz*, *Jones*, and *Kyllo* precluded any claims that property rights were "'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate."[46] Because *Carpenter* did not involve a physical trespass, such statements remain dicta.

Resolution of whether trespass is sufficient to constitute a Fourth Amendment violation is not critical to our argument. For our purposes, it is enough that the propriety of the conduct of law enforcement officials' actions remains a consideration in the Fourth Amendment analysis.

2. The Enablement of Indiscriminate, Dragnet Searches (Factor 1B)

Other discussions by the Court focused on particular law enforcement practices as a general matter, especially when the search permits what the Court called in *United States v. Di Re*[47] a "too permeating police surveillance."[48] Consistent with the hostility toward general warrants, the Court has expressed skepticism about dragnet practices that sweep everything without suspicion.

The issue was raised most notably in *Knotts*, where the Court saw no need to address the constitutionality of "dragnet type law enforcement practices" that permit "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision" given that the conduct in question did not rise to that level.[49] The affirmative act of reserving this question raised the possibility that the Court would find conduct that reached that level constitutionally problematic if presented with it in a future case.

The Court eventually reached this issue when ruling a search unconstitutional in *Jones*, in which the majority characterized GPS tracking as the type of "dragnet-type law enforcement practices" that were not presented in *Knotts*.[50] The separate opinions authored by Justices Sotomayor and Alito (which together represented a majority of the Court) raised similar concerns about other technologies that permit more comprehensive tracking of a person's movements.[51]

The Court confronted an even more comprehensive form of surveillance in *Carpenter*. The Court repeated *Di Re*'s observation

45. *Id.* at 2213–14, 2214 n.1.

46. *Id.* at 2214 n.1 (disagreeing with *id.* at 2224, 2227–28); *id.* at 2235–36, 2244–46 (Thomas, J., dissenting); *id.* at 2264–66 (Gorsuch, J., dissenting).

47. 332 U.S. 581 (1948).

48. *Id.* at 595.

49. United States v. Knotts, 460 U.S. 276, 283–84 (1983).

50. United States v. Jones, 565 U.S. 400, 409 n.6 (2012) (citing *Knotts*, 460 U.S. at 284).

51. *Id.* at 415–17 (Sotomayor, J., concurring); *id.* at 428–31 (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

that the Fourth Amendment was designed "to place obstacles in the way of a too permeating police surveillance."[52] The Court noted that five Justices raised the concerns in *Jones* that the use of devices (including cell phones) to track a person's every movement would violate the Fourth Amendment.[53] Like the four weeks of GPS tracking information at issue in *Jones*, the eighteen weeks of cell site location information (CSLI) at issue in *Carpenter* provided a detailed and inexpensive record about the defendant's movements that is tantamount to "near perfect surveillance."[54] More problematically, in contrast to the GPS tracking device in *Jones*, which recorded a single defendant's movements on a going-forward basis after the device had been installed, CSLI permits retrospective reconstruction of a person's movements going back five years for everyone carrying a cell phone.[55] In so holding, the Court rejected Justice Kennedy's claims that these practices did not constitute dragnet-type practices.[56]

Thus, when it comes to practices that permit the collection of the type of comprehensive, untargeted searches associated with dragnet tactics, the Court has invalidated them without any analysis of the particular circumstances in which they were employed.

B. The Defendant Conduct Factor (Factor 2)/Fairness to the Defendant

The second factor turns not on evidence of the conduct of law enforcement but rather on the conduct of the defendant. Examining the extent to which defendants themselves made information available invokes values that are quite different from abuse by law enforcement officials. Instead, focusing on defendants' conduct implicates concerns that sound in fairness by requiring defendants to bear the risks they have voluntarily assumed.

1. Exposure by the Defendant (Factor 2A)

The Court has long looked to the defendant's conduct in determining whether a Fourth Amendment violation has occurred. As the Court noted in *Katz*, the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public."[57]

Knowing exposure forms the basis of four distinct lines of Fourth Amendment jurisprudence. The first is the plain view doctrine first articulated by the Court in *Hester v. United States*,[58] which upheld

52. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

53. *Id.* at 2215 (citing *Jones*, 565 U.S. at 415); *Jones*, 565 U.S. at 426, 430 (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

54. *Carpenter*, 138 S. Ct. at 2210, 2218.

55. *Id.* at 2218.

56. *Id.* at 2215 n.2.

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

58. 265 U.S. 57 (1924).

the admissibility of a jug the defendant had dropped, a bottle he had tossed away, and a jar that he had thrown from the house, all of which contained moonshine.[59] In a two-paragraph opinion, Justice Holmes held that evidence disclosed by the acts of the defendant and his associates were neither products of a search nor a seizure.[60] The Court has similarly invoked the plain view doctrine to uphold the admissibility of evidence observed from aircraft without protection from airborne observation,[61] merchandise displayed for public sale,[62] observations of the tire tread and foreign paint samples obtained from the exterior of a car,[63] and a bag containing contraband held by a person standing in the doorway of her house.[64] The persistence of the open fields doctrine makes clear that plain view is not purely a matter of property law and is better understood in terms of defendants' expectations of the significance of their conduct.[65]

The second is the misplaced trust doctrine established by a series of pre-*Katz* decisions upholding the admissibility of information revealed to a confidential informant whom defendants mistakenly believe will keep their secrets.[66] The Court concluded in *United States v. White*[67] that the *Katz* reformulation around the reasonable expectations of privacy did not change this conclusion. Although these defendants may have held a subjective expectation of privacy, the unavoidable possibility that a trusted colleague may reveal the defendant's confidences to law enforcement renders any expectations of privacy objectively unreasonable.[68]

The third is the third-party doctrine, established by a pair of post-*Katz* decisions holding that any information revealed to others is unprotected by the Fourth Amendment.[69] Citing the Court's misplaced trust decisions as precedent, these decisions made clear

---

59. *Id.* at 58.

60. *Id.*

61. California v. Ciraolo, 476 U.S. 207, 213 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 235 (1986); Florida v. Riley, 488 U.S. 445, 449 (1989) (plurality opinion).

62. Maryland v. Macon, 472 U.S. 463, 469 (1985).

63. Cardwell v. Lewis, 417 U.S. 583, 591 (1974).

64. United States v. Santana, 427 U.S. 38, 40, 42 (1976).

65. Kyllo v. United States, 533 U.S. 27, 33 (2001); *see also supra* note 34 and accompanying text.

66. Hoffa v. United States, 385 U.S. 293, 302–03 (1966) (upholding the admissibility of confidential informant's direct testimony); Lewis v. United States, 385 U.S. 206, 207 (1966) (same). Evidence of information revealed to third parties may also be introduced by testimony of law enforcement officials listening to the conversation via electronic surveillance. Lopez v. United States, 373 U.S. 427, 440 (1963); On Lee v. United States, 343 U.S. 747, 754 (1952).

67. 401 U.S. 745 (1971) (plurality opinion).

68. *Id.* at 752.

69. Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

that any such information falls outside defendants' subjective and objective expectations of privacy.[70]

The fourth is the Court's jurisprudence on searches of shared spaces, which also indicates that the act of occupying a shared space with others lessens an individual's expectation of privacy because the individual assumes some of the risk. In *United States v. Matlock*,[71] the Court held that law enforcement can receive permission to search a shared area from someone with common authority because the individuals sharing the area "assumed the risk that one of their number might permit the common area to be searched."[72] In *Illinois v. Rodriguez*,[73] the Court also upheld that individuals who share a space have a decreased expectation of privacy based on a similar assumption of the risk standard.[74] Much like the plain view doctrine, the defendant's conduct in occupying a shared space lessens her expectations of privacy.

The Court grounded all four doctrines in the defendant's assumption of the risk. Concerning misplaced trust, *Lopez v. United States*[75] held that "the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court."[76] The Court would reiterate in *Hoffa v. United States*[77] that the defendant "was relying upon his misplaced confidence that [the confidential informant] would not reveal his wrongdoing" and that both the majority and dissents in *Lopez* were unanimous in agreeing that the risk of disclosure is a risk that every speaker assumes.[78] In *United States v. White*, the plurality opined that "one contemplating illegal activities must realize and risk that

70. *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443.

71. 415 U.S. 164 (1974).

72. *Id.* at 171 n.7.; Georgia v. Randolph, 547 U.S. 103, 111 (2006) ("As *Matlock* put it, shared tenancy is understood to include an 'assumption of risk,' on which police officers are entitled to rely . . . .").

73. 497 U.S. 177 (1990).

74. *Id.* at 194 (Marshall, J., dissenting) (an individual "relinquishe[s] some of his expectation of privacy by sharing or control over his property with another person").

75. 373 U.S. 427 (1963).

76. *Id.* at 439. Justice Brennan's dissent concurred, noting that the defendants in both *On Lee* and *Lopez* "assumed the risk that his acquaintance would divulge their conversation" and that "[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak." *Id.* at 450, 465 (Brennan, J., dissenting). Although he raised this point as part of his effort to distinguish direct from electronic eavesdropping, the Court rejected that distinction as "amount[ing] to saying that he has a constitutional right to rely on possible flaws in the agent's memory." *Id.* at 439.

77. 385 U.S. 293 (1966).

78. *Id.* at 302–03.

his companions may be reporting to the police," that "the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent," and that every "defendant necessarily risks" the revelation of conversations with other people regardless of whether revealed by the informant's testimony or by a recording of the conversation.[79] Justice Black provided the critical fifth vote on the grounds that *Katz* was wrongly decided.[80] Any lingering doubts created by the absence of a majority opinion in *White* were obviated by *United States v. Jacobsen*, in which a clear majority acknowledged that "[i]t is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."[81] A parallel line of decisions similarly held that defendants who share control of bags and residences assume the risk that their cotenants may consent to a search.[82]

The Court similarly made assumption of the risk the basis of the third-party doctrine. For example, *Miller* cited the misplaced trust cases for the proposition that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[83] *Smith* adopted the same approach, relying on the misplaced trust cases and the above-quoted language from *Miller* to support the proposition that dialing a phone number "'exposed' that information" to the telephone company and that "[i]n so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[84]

Assumption of the risk was later adopted as the rationale for plain view as well. For example, *Knotts* followed that anyone driving on public streets "voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[85] Per *Smith*, anyone making voluntary conveyances and exposure of

79. United States v. White, 401 U.S. 745, 751–52 (plurality opinion).

80. *Id.* at 754 (Black, J., concurring in the judgment). Justice Brennan agreed that *Katz* did not apply retroactively but joined the three dissenters in concluding that *Katz* mandated that *On Lee* and *Lopez* be overruled. *Id.* at 755 (Brennan, J., concurring in the result).

81. United States v. Jacobsen, 466 U.S. 109, 117 (1984).

82. United States v. Matlock, 415 U.S. 164, 177 (1974) (shared residence); Frazier v. Cupp, 394 U.S. 731, 740 (1969) (shared bag). Later decisions have made clear that the consent of one coresident is not sufficient when the other coresident is present and objects. Georgia v. Randolph, 547 U.S. 103, 113 (2006). A coresident's consent is sufficient if the objecting coresident is removed for objectively valid reasons. Fernandez v. California, 571 U.S. 292, 306 (2014).

83. United States v. Miller, 425 U.S. 435, 443 (1976).

84. Smith v. Maryland, 442 U.S. 735, 744 (1979).

85. United States v. Knotts, 460 U.S. at 276, 281–82 (1983).

information assumed the risk that the information may be revealed.[86] The dissent also found this rationale implicit in *Ciraolo*, which "assume[d] that the Court believes that citizens bear the risk that air travelers will observe activities occurring within backyards that are open to the sun and air."[87]

The doctrine of assumption of the risk originated in tort law.[88] Closely related to (but distinct from) contributory negligence[89] and consistent with the ancient maxim from Roman law, *volenti non fit injuria* (to a willing person, injury is not done),[90] assumption of the risk arose out of the policy that people who know that certain conduct carries risks and nonetheless elect to proceed with that conduct should not later be heard to complain about harms resulting from their decision.[91] The emergence of comparative negligence,[92] statutes such as workers' compensation laws and the Federal Employers' Liability Act,[93] and complications arising from the fact that the doctrine represented a complete defense have led tort law to largely abandon it.[94] These developments are unique to tort law and, therefore, do not affect the Fourth Amendment analysis.

The Supreme Court imposed some limitations on both the third-party doctrine and the assumption of the risk rationale in *Carpenter*. Although the Court recognized that *Knotts*, *Smith*, and *Miller* rested on knowing exposure and assumption of the risk,[95] it declined to follow those precedents, noting that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere."[96] As we will explain in further detail when discussing the next factor, *Carpenter* held that courts must balance the fact that the defendant revealed information voluntarily against the sensitivity of the information revealed.[97] In so holding, the *Carpenter* majority did not eliminate the conduct of the defendant as a consideration to weigh in the Fourth Amendment balance. On the contrary, treating it as one factor that must be weighed against other considerations explicitly

86. *Id.* at 283 (quoting *Smith*, 442 U.S. at 744–45).

87. California v. Ciraolo, 476 U.S. 207, 223 (1986) (Powell, J., joined by Brennan, Marshall & Blackmun, JJ., dissenting).

88. RESTATEMENT (FIRST) OF TORTS § 893 (AM. L. INST. 1939).

89. RESTATEMENT (SECOND) OF TORTS § 496A cmt. d. (AM. L. INST. 1965).

90. *Id.* § 496A cmt. b.

91. *Id.* § 496C cmt. b.

92. DAN B. DOBBS ET AL., THE LAW OF TORTS § 237 (2d ed. 2011).

93. *Id.* § 235; *see also* Norfolk S. Ry. Co. v. Sorrell, 549 U.S. 158, 166, 168, 171 (2007).

94. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § 3 cmt. c (AM. L. INST. 2000); DOBBS ET AL., *supra* note 92, § 237.

95. Carpenter v. United States, 138 S. Ct. 2206, 2215–16 (2018).

96. *Id.* at 2217.

97. *See infra* Section I.C.

reaffirmed its relevance.[98] The enduring importance of the conduct of the defendant is underscored by the fact that *Carpenter* declined to overrule *Miller* or *Smith*.[99] Interestingly, the dissents offered divergent criticisms of the majority's decision to qualify the assumption of the risk rationale: Justice Kennedy would have adhered to it,[100] while Justice Gorsuch would have abandoned it altogether.[101]

2. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B)

Assumption of the risk has always been subject to two important constraints: Specifically, people can be said to have assumed risks only if they knew about them[102] and if their acceptance of them was voluntary.[103] Both constraints found their way into Fourth Amendment doctrine as well.

a. Technology and Knowledge

As noted above, assumption of the risk applies only to risks known to the person said to have assumed them. Although the *Second Restatement of Torts* treated this as a subjective inquiry,[104] decisions applying the doctrine began applying an objective test to bring it in line with the emerging principles of comparative negligence.[105]

The Supreme Court incorporated a version of this objective test into the reasonable-expectations-of-privacy prong of *Katz*.[106] It particularly informed the Court's Fourth Amendment decisions involving technology. The Court has recognized that "[n]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them."[107] For example, in *Ciraolo*, the Court was asked to determine whether the defendant's marijuana plants were protected from aerial

98. *Carpenter*, 138 S. Ct. at 2231 (Kennedy, J., joined by Thomas & Alito, JJ., dissenting).

99. *Id.* at 2220 (majority opinion).

100. *Id.* at 2227 (Kennedy, J., dissenting).

101. *Id.* at 2263 (Gorsuch, J., dissenting).

102. RESTATEMENT (SECOND) OF TORTS, *supra* note 89, §§ 496C, 496D.

103. *Id.* §§ 496C, 496E.

104. *Id.* § 496D cmt. c.

105. DOBBS ET AL., *supra* note 92, § 236.

106. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Although the original *Katz* included separate subjective and objective requirements, *id.* at 361, the subjective inquiry is now regarded as irrelevant, *see* Carpenter v. United States, 138 S. Ct. 2206, 2238 (2018) (Thomas, J., dissenting) (citing Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015)).

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

observation.[108] The Court held that the Fourth Amendment did not protect any evidence visible to the naked eye, but the Court's reasoning examined the defendant's conduct through the lens of reasonable expectations: "In an age where private and commercial flight in the public airways is routine, it is unreasonable for [the defendant] to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."[109] The defendant's conduct was unreasonable because commercial aerial observation had become "routine" by the 1980s when this case was decided.[110]

Consistent with this principle, the Court has upheld the use of normal sensory enhancement technologies, such as magnification devices,[111] illumination equipment,[112] and recording devices.[113] *Ciraolo* and *Dow Chemical Co. v. United States*, both decided on the same day, added to this list aerial observation points so long as they are sufficiently common to put the defendant on effective notice.[114] At the same time, however, the *Dow Chemical* Court reserved the possibility that the use of "some unique sensory device that, for example, could penetrate the walls of buildings and record conversations" or "highly sophisticated surveillance equipment not generally available to the public, such as satellite technology," might present a different case.[115]

The Court confronted this possibility in *Kyllo v. United States*,[116] in which it held that the use of a thermal imager from the public street to examine the heat emanating from a house violated the Fourth Amendment.[117] In so holding, the Court emphasized that the technology at issue was "not in general public use"[118] and "not 'routine,'"[119] although, as we shall discuss in the next Section, the fact

108. California v. Ciraolo, 476 U.S. 207, 213 (1986).
109. *Id.* at 215.
110. *Id.*
111. On Lee v. United States, 343 U.S. 747, 754 (1952) (dictum); United States v. Lee, 274 U.S. 559, 563 (1927) (dictum); *Knotts*, 460 U.S. at 282–83 (quoting *Lee*, 274 U.S. at 563, with approval).
112. Texas v. Brown, 460 U.S. 730, 739–40 (1983); *Lee*, 274 U.S. at 563; *Knotts*, 460 U.S. at 282–83 (quoting *Lee*, 274 U.S. at 563, with approval).
113. *On Lee*, 343 U.S. at 753–54.
114. *Ciraolo*, 476 U.S. at 215; Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (holding that the use of "a *conventional*, albeit precise, commercial camera *commonly used* in mapmaking" was constitutionally unproblematic (emphasis added)).
115. *Dow Chem. Co.*, 476 U.S. at 238.
116. 533 U.S. 27 (2001).
117. *Id.* at 40.
118. *Id.* at 34.
119. *Id.* at 40 n.6.

that the surveillance was being conducted on a home also played a role in the analysis.[120]

b. Technology and Voluntariness

In addition, assumption of the risk traditionally carries with it the requirement that the risks be voluntarily accepted.[121] This inquiry turns on the availability of reasonable alternatives.[122] The Court's willingness to recognize this limitation has varied over time. For example, the majority in *Smith v. Maryland*[123] held that anyone placing a phone call voluntarily assumed the risk that the phone number called would be revealed despite the dissent's objection that "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[124] The dissent further noted, "Implicit in the concept of assumption of the risk is some notion of choice," and the telephone had become by that time "a personal or professional necessity."[125] Thus, the Court's holding "ignores the vital role telephonic communication plays in our personal and professional relationships."[126] Similarly, the Court held in *California v. Greenwood*[127] that people have no reasonable expectation of privacy in trash left outside their homes even when, as the dissent noted, they are legally obligated to dispose of their trash in this manner.[128]

The Court's more recent decisions have taken concerns about voluntariness more seriously. Specifically, although *Carpenter* recognized that *Knotts*, *Smith*, and *Miller* rested on voluntary conveyance and assumption of the risk,[129] it rejected the idea that cell phone users voluntarily expose their location information to their providers in part because cell phones have become so indispensable that people "compulsively carry cell phones with them all the time" to the point where it is "almost a 'feature of human anatomy.'"[130] In addition, cell phones disclose location information without any affirmative act by users.[131] "As a result, in no meaningful sense does

120. *See infra* Section I.C.1.
121. *See supra* note 86 and accompanying text.
122. RESTATEMENT (SECOND) OF TORTS, *supra* note 89, § 496E; DOBBS ET AL., *supra* note 92, § 236.
123. 442 U.S. 735 (1979).
124. *Id.* at 750 (Marshall, J., dissenting).
125. *Id.* at 749–50.
126. *Id.* at 751.
127. 486 U.S. 35 (1988).
128. *Id.* at 54–55 (Brennan, J., dissenting).
129. Carpenter v. United States, 138 S. Ct. 2206, 2215–16 (2018).
130. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).
131. *Id.* at 2220.

the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[132]

Examination of the conduct of defendants implicates values that are quite different from the examination of the conduct of law enforcement officials. Rather than trying to emphasize governmental abuse, this inquiry focuses on issues of fairness.

C. The Information Sensitivity Factor (Factor 3)/Protection of the Substantive Privacy Interests of the Defendant

A third factor focuses neither on the conduct of law enforcement nor on the conduct of defendants in exposing their information but turns on evidence of the nature of the information gleaned from a search.[133] Although *Boyd* famously observed that the Fourth Amendment protects "the privacies of life,"[134] the nature of the information itself has largely remained on the periphery of Fourth Amendment analysis.[135] Early cases relied on the home as a per se rule that protected the sensitivity of information that could be collected there. As technology improved the ability to conduct surveillance on defendants' activities, more modern cases used location information as a proxy for the sensitivity of the information that surveillance could reveal. Most recently, the Court has begun to engage in more direct analysis of the sensitivity of the information, epitomized by *Riley v. California*.[136] In so doing, the Court focused not on fairness to defendants or the avoidance of governmental abuse but rather on the substantive privacy issues at stake.

1. The Sensitivity of the Home

The most persistent per se rule that the Court has used to identify when a search might reveal sensitive information is to consider whether the location being searched is the defendant's home. At times, the Court based the significance of the home on the fact that it specifically appears in the text of the Fourth Amendment.[137]

On other occasions, the Court has invoked the home as a proxy for the sensitivity or intimacy of the information. Reliance on the home as a proxy can be traced back to the pre-Revolutionary English precedents. In *Entick v. Carrington*,[138] which the Court has credited

132. *Id.* (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1975)).

133. For an earlier, somewhat skeptical argument about the merits of focusing on the private nature of the information collected by the government, see Kerr, *supra* note 1, at 512–15, 534–35.

134. Boyd v. United States, 116 U.S. 616, 630 (1886).

135. Ohm, *supra* note 13, at 372.

136. 573 U.S. 373 (2013).

137. U.S. CONST. amend. IV (referring to "[t]he right of the people to be secure in their . . . houses").

138. 19 Howell's St. Tr. 1029, 95 Eng. Rep. 807 (K.B. 1765).

as explaining the motivation for the Fourth Amendment, Lord Camden ruled against a warrant that had authorized the government to take papers from Entick's home.[139] In *Boyd*, the Court discusses Camden's judgment in *Entick* at length and clarifies that the offense in *Entick* stemmed from "the invasion of [one's] indefeasible right of personal security, personal liberty, and private property."[140] This principle is reaffirmed in the decision in *Boyd*.[141] This underscores that the importance of the home has long been a proxy in the Fourth Amendment analysis for our desire to protect sensitive information from government reach. Pre-*Katz* Supreme Court cases similarly gave the home more extensive Fourth Amendment protection because it was a "constitutionally protected area."[142]

This primacy of the home was called into question by the Court's landmark decision in *Katz v. United States*, which observed that "the correct solution of Fourth Amendment problems is not necessarily promoted by the incantation of the phrase 'constitutionally protected area'" and rejected claims "that this concept can serve as a talismanic solution to every Fourth Amendment problem."[143] The rejection of the significance of particular locations is embodied most forcefully in *Katz*'s enduring declaration that "the Fourth Amendment protects people, not places."[144]

Although this statement reads like an authoritative declaration against according constitutional significance to any particular location, the Court's jurisprudence belies such a conclusion. For example, Justice Harlan's concurrence in *Katz* continued to recognize that the "home is, for most purposes, a place where [one] expects privacy."[145] Moreover, the Court's post-*Katz* decisions continued to extend special solicitude to the home. The Court relied on the fact that the beeper at issue in *Karo* revealed information inside the home to distinguish it from the beeper at issue in *Knotts*, holding that "[a]t the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental

139. *Boyd*, 116 U.S. at 626–27 ("As every American statesmen, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom, . . . 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.").

140. *Id.* at 630. See also Clancy, *supra* note 7, at 985–90, for a general discussion of *Boyd*, *Entick*, and the English and Colonial roots of the importance of the home as proxy for sensitive information.

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

142. *See, e.g.*, Berger v. New York, 388 U.S. 41, 44, 52, 57, 59 (1967); Hoffa v. United States, 385 U.S. 293, 301 (1966); Lopez v. United States, 373 U.S. 427, 438–39 (1963); Silverman v. United States, 365 U.S. 505, 510, 512 (1961).

143. Katz v. United States, 389 U.S. 347, 350, 351 n.9 (1967).

144. *Id.* at 351.

145. *Id.* at 361 (Harlan, J., concurring).

intrusion not authorized by a warrant."[146] The Court similarly distinguished the aerial surveillance in *Dow Chemical* from that in *Ciraolo* by noting that "[t]he intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant."[147] *Oliver v. United States* contrasted open fields with the "intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"[148] *United States v. Dunn*[149] similarly found the special protections extended to homes to not apply to a "barn [that] was not being used for intimate activities of the home."[150] *Florida v. Jardines* extended greater protection against the use of drug-sniffing dogs near the home than it did in airports or during lawful traffic stops.[151] As the Court succinctly concluded, "[W]hen it comes to the Fourth Amendment, the home is first among equals."[152]

The Court offered its most complete exposition of this conclusion in *Kyllo v. United States*, which made clear that the Court protected the home as a proxy for the intimacy of the information even against emanations of heat that were clearly visible from the public street.[153] What mattered was not only how the information was gathered but also that the content of the information was about the interior of a home. In addition to reaffirming the phrase, "constitutionally protected area,"[154] the Court held that "the Fourth Amendment draws 'a firm line at the entrance to the house'"[155] and that "[i]n the home, our cases show, *all* details are intimate details."[156] To hold otherwise would require the Court "to develop a jurisprudence specifying which home activities are 'intimate' and which are not."[157] This the Court declined to do because "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[158] This analysis indicates that the Court is

146. United States v. Karo, 468 U.S. 705, 714 (1984).

147. Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986); *accord id.* at 237 n.4 (finding it "important [that] this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened").

148. Oliver v. United States, 466 U.S. 170, 180 (1984) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); *accord* United States v. Dunn, 480 U.S. 294, 307 (1987) (quoting *Oliver*, 466 U.S. at 180).

149. 480 U.S. 294 (1987).

150. *Id.* at 302.

151. Florida v. Jardines, 569 U.S. 1, 10–11 (2013).

152. *Id.* at 6.

153. Kyllo v. United States, 533 U.S. 27, 35–36 (2001).

154. *Id.* at 34.

155. *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

156. *Id.* at 37.

157. *Id.* at 38–39.

158. *Id.* at 37.

relying on a per se rule that treats all activities in the home as sufficiently intimate to demand protection.

2. The Sensitivity of Location Information

In addition to the home, the Court has placed particular emphasis on location information. For example, the *Knotts* Court indicated that the continuous tracing of a person's location might be constitutionally problematic.[159] The connection between location information and intimate, personal information was drawn more explicitly by Justice Sotomayor's concurrence in *Jones*, in which she warned about "generat[ing] a precise, comprehensive record of a person's public movements."[160] Justice Alito, joined by three other Justices, raised similar concerns.[161]

A majority of the Court endorsed these concerns in *Carpenter*, which acknowledged that it had "already shown special solicitude for location information in the third-party context."[162] It noted that *Knotts* "was careful to distinguish between the rudimentary tracking facilitated by the beeper [at issue in that case] and more sweeping modes of surveillance," which might amount to "twenty-four hour surveillance of any citizen."[163] *Carpenter* further observed that five Justices in *Jones* had similarly warned about the dangers of long-term tracking of every movement a person makes in a vehicle.[164] Consistent with these concerns, the Court raised concerns about "the unique nature of cell phone location records,"[165] which can give law enforcement access to location information that is "detailed, encyclopedic, and effortlessly compiled"[166] and to "an all-encompassing record of the holder's whereabouts," complete with timestamps.[167] Such "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years . . . implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[168]

Together, these decisions make clear that the Court regards comprehensive tracking of a person's movements as an impermissible intrusion into information that people regard as intimate.

---

159. *See* United States v. Knotts, 460 U.S. 276, 283 (1983).

160. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

161. *See id.* at 428–30 (Alito, J., joined by Ginsburg & Breyer, JJ., concurring in the judgment).

162. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

163. *Id.* at 2215 (quoting *Knotts*, 460 U.S. at 283–84).

164. *Id.* (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *id.* at 430 (Alito, J., concurring)).

165. *Id.* at 2217.

166. *Id.* at 2209.

167. *Id.* at 2217.

168. *Id.* at 2220.

3. Direct Analysis of Information Sensitivity

In addition to relying on the home and location information as proxies, the Supreme Court has directly analyzed the sensitivity of information revealed in the search. This mode of analysis traces its roots to *Boyd*'s observation that the Fourth Amendment was intended to protect "the privacies of life"[169] and Justice Brandeis's *Olmstead* dissent cautioning about new technologies that would permit access to a person's "unexpressed beliefs, thoughts, and emotions."[170] *Dow Chemical* similarly speculated about the dangers of future technologies that would allow law enforcement "to hear and record confidential discussions,"[171] and its companion decision in *Ciraolo* implicitly credited concerns about technologies that revealed "intimate associations, objects, or activities otherwise imperceptible to police or fellow citizens."[172]

Justice Sotomayor's *Jones* concurrence raised similar concerns about the collection of data that "reflect[] a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."[173] When technologies permit "the Government to ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on," it does not matter whether that information was collected in an otherwise legal manner.[174] Justice Alito's concurrence observed that the ease with which law enforcement can now collect location information eliminated the practical protections for people's privacy.[175] The result was that the collection of information was more revealing, even if it represented nothing more than a scaled-up version of traditional surveillance.[176]

The Court offered its most fulsome discussion of the importance of the sensitivity of the information in *Riley v. California*, in which the Court held that warrantless searches of digital information on a cell phone seized during an arrest violated the Fourth Amendment.[177] Importantly, the Court went beyond the considerations demanded by

169. Boyd v. United States, 116 U.S. 616, 630 (1886).

170. Olmstead v. United States, 277 U.S. 400, 474 (1928) (Brandeis, J., dissenting).

171. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

172. California v. Ciraolo, 476 U.S. 207, 215 n.3 (1986).

173. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

174. *Id.* at 416.

175. *Id.* at 429 (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

176. *Id.*; *accord* U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989) (applying the privacy exception to the Freedom of Information Act to block disclosure of dossiers of prior convictions compiled from public sources because doing so would eliminate "the practical obscurity of rap-sheet information").

177. Riley v. California, 573 U.S. 373, 386 (2014).

its precedents on searches incident to arrest to engage in direct analysis of the privacy of the information at stake. In short, cell phones are "minicomputers" with "immense storage capacity" capable of storing an amazing breadth of information, including text, pictures, videos, browsing history, calendars, and contacts lists.[178] Placing all of these myriad types of information in one place allows the reconstruction of "[t]he sum of an individual's private life" going back to the purchase date of the phone or beyond.[179] People's tendency to carry their phones with them means that people now carry with them "a digital record of nearly every aspect of their lives—from the mundane to the intimate" at all times.[180]

In addition to the greater quantity of information, cell phones contain types of data that are "qualitatively different."[181] Information about owners' internet search and browsing history, historical location information, and the apps they use "together can form a revealing montage of the user's life."[182] As a result,

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form . . . .[183]

Far from being "just another technological convenience," modern cell phones now "hold for many Americans 'the privacies of life.'"[184]

Carpenter echoed the sentiments raised in Justice Sotomayor's *Jones* concurrence and *Riley* when it recognized that CSLI "provides an intimate window into a person's life, revealing his . . . 'familial, political, professional, religious, and sexual associations'" and "the privacies of life."[185] Furthermore, *Carpenter*'s recognition that "[a] person does not surrender all Fourth Amendment protection by

---

178. *Id.* at 393.
179. *Id.* at 394–95.
180. *Id.* at 395.
181. *Id.*
182. *Id.* at 396. As the Court explains,

> There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely.

Id.
183. *Id.* at 396–97.
184. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
185. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (first quoting Unites States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); and then quoting *Boyd*, 116 U.S. at 630).

venturing into the public sphere" makes clear that the sensitivity of the information could trump the manner in which it was collected.[186] This was further confirmed by *Carpenter*'s core holding that the revelation to third parties could be counterbalanced by the sensitivity of the information.[187]

This direct analysis of the sensitivity of the information represents a new dimension to the Supreme Court's Fourth Amendment jurisprudence. It represents a mode of analysis that is more directly focused on defendants' privacy interests than consideration of the conduct of law enforcement or any acts by the defendants that may have revealed particular information. The Court makes clear that this consideration is independent of the manner in which the information is obtained. The Court's explicit embrace of the quantity as well as the quality of information goes well beyond the proxy models upon which the Court previously relied to instead focus on the real-world import of the information.

D. The Societal Impact Factor (Factor 4)/Aggregate Social Welfare

The fourth factor reflected in the Supreme Court's Fourth Amendment jurisprudence focuses on the impact of law enforcement surveillance on society as a whole. This mode of analysis emphasizes aggregate social welfare instead of individual rights. This consists of two countervailing considerations: the impact on the effectiveness of law enforcement and the types of second-order compensations that expanded surveillance has on individual citizens. Although this factor has the least representation in Supreme Court decisions of the four factors that we identify, we suspect that it will grow in importance in the coming years.

1. The Social Benefits of More Effective Law Enforcement (Factor 4A)

The Supreme Court has long maintained an ambivalent posture toward practices that make law enforcement more effective. Though the first factor focusing on the conduct of law enforcement recognizes that the goal of the Fourth Amendment is to protect "the privacies of life" against "arbitrary power,"[188] the Court has also been clear that the motivation for the Fourth Amendment was to "restrain the abuse, . . . not abolish the power."[189] Undoubtedly, this is because reasonable searches are an important mechanism for law enforcement to investigate crime. Indeed, both sides of this tension were apparent in *Carpenter*. The majority opinion emphasized the importance of "plac[ing] obstacles in the way of a too permeating

186. *Id.*
187. *Id.* at 2219–20.
188. *Boyd*, 116 U.S. at 630.
189. *Id.* at 641 (Waite, C.J. & Miller, J., concurring).

police surveillance,"[190] while Justice Kennedy's dissent expressed the concern that the Court's decision "limits the effectiveness of an important investigative tool for solving serious crimes."[191]

The Court's decisions have thus balanced concerns about abuse of government power identified in the first factor we discuss against society's interest in effective law enforcement. For example, in *King v. Maryland*,[192] the Court explicitly balanced the effectiveness of law enforcement against the Fourth Amendment considerations captured in the other three factors we identify, writing that "a government interest [in investigating crimes] does not alone suffice to justify a search," but rather the "government interest must outweigh the degree to which the search invades an individual's legitimate expectation of privacy."[193] Similarly, in *Riley v. California*, the Court took into account the "impact on the ability of law enforcement to combat crime" when it held that law enforcement must get a warrant before searching a cell phone seized incident to an arrest.[194]

Technological improvements can also allow law enforcement to investigate crime more efficiently. The Court has held that the collection of information that was legal is not rendered illegal solely because of technological developments that made that information easier or cheaper to collect. For example, the Court acknowledged in *Smith v. Maryland* that if defendants have no legitimate expectation of privacy to a phone number conveyed to an operator, they do not gain additional protections simply "because the telephone company has decided to automate."[195] The Court similarly held in *United States v. White* that statements made to a confidential informant are not rendered inadmissible just because law enforcement officials use technology to make a "rendition of what a defendant has said" that is more "accurate and reliable" than "the unaided memory of a police agent."[196] *Knotts* similarly held that if law enforcement officials could have followed the defendant's car along the public streets, nothing in the Fourth Amendment prevented them from using technology to do so.[197] The *Knotts* Court further held that "[i]nsofar as respondent's

190. *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

191. *Id.* at 2233 (Kennedy, J., joined by Thomas & Alito, JJ., dissenting).

192. 569 U.S. 435 (2013).

193. *Id.* at 461. This factor is also weighed in the dissent in *King*, where Justice Scalia writes that "[s]olving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches." *Id.* at 481 (Scalia, J., dissenting).

194. Riley v. California, 573 U.S. 373, 401 (2014) ("We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime.").

195. Smith v. Maryland, 442 U.S. 735, 745 (1979).

196. United States v. White, 401 U.S. 745, 753 (1971) (plurality opinion).

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

complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now."[198]

On the other hand, the Court has found investigatory practices that reveal too much information constitutionally problematic. As the Court recognized in *Riley v. California*, the requirements of the Fourth Amendment are "not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[199] The Court thus recognized that its "decision today will have an impact on the ability of law enforcement to combat crime."[200] Simply put, "privacy comes at a cost."[201]

Justice Alito, joined by three other Justices, raised similar concerns in *Jones* about how law enforcement's ever-increasing ability to collect information eventually raises constitutional problems.[202] The Court offered a similar observation in *Carpenter*, further noting that privacy sometimes requires erecting "obstacles in the way of a too permeating police surveillance" even when giving police greater latitude would enable them to solve more crimes.[203]

The situation may be different when a technological advancement does not just make certain investigatory practices more effective or less expensive but actually makes it possible to solve crimes that were previously nearly impossible to solve. Interestingly, this dimension comes to the Fourth Amendment by way of a statute. In the aftermath of *Katz*, Congress enacted legislation requiring law enforcement that wanted to deploy a wiretap to satisfy a higher standard than the Fourth Amendment required.[204] Indeed, the judicial approvals needed to authorize a wiretap under this statute are sometimes called "superwarrants."[205] Specifically, the statute requires the judge issuing the superwarrant to determine whether "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too

198. *Id.* at 284.

199. *Riley*, 573 U.S. at 401 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

200. *Id.*

201. *Id.*

202. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment).

203. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

204. 18 U.S.C. § 2518(3).

205. *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620, 630, 645 (2003); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1561 (2004).

dangerous."[206] In short, the fact that a crime may be difficult or impossible to solve without the wiretap became one of the considerations a judge must weigh when deciding whether to permit it to be employed.

Although this statutory requirement was imposed for audio surveillance, Congress has not enacted any parallel restrictions on video surveillance, which, in the absence of legislation, is limited only by the Fourth Amendment. Lower courts confronted with this vacuum have incorporated this statutory requirement into the Fourth Amendment standard governing video surveillance.[207] This suggests that the Fourth Amendment allows greater latitude for investigative techniques for crimes that would otherwise be difficult or impossible to solve. As we shall see, this may apply to biometric technologies like the use of DNA, which have the potential to both convict and exonerate defendants in cases where definitive proof would be otherwise impossible without the use of such technologies.[208]

2. The Social Costs of Avoidance Behavior (Factor 4B)

Recognizing the legality of a particular form of surveillance is not likely to be the end of the story. Potential defendants subject to a certain type of scrutiny have strong incentives to evade it either by foregoing certain conduct or by undertaking affirmative steps to avoid detection or to obscure their behavior.[209] These avoidance tactics, in turn, prompt law enforcement to take further actions in an attempt to counteract these evasions.[210] The net sum of these moves and countermoves creates social costs that, on balance, may be harmful to

206. 18 U.S.C. § 2518(3)(c).

207. *See, e.g.*, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986); United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984); *see also* United States v. Williams, 124 F.3d 411, 416 (3d Cir. 1997) (assuming the applicability of this requirement without adopting it).

208. The Court has mentioned the potential benefit of using DNA to solve crimes more accurately, writing, "[I]n the interests of justice, identifying an arrestee as the perpetrator of some heinous crime may have the salutary effect of freeing a person wrongfully imprisoned." King v. Maryland, 569 U.S. 435, 437 (2013). Though this analysis was not dispositive in the ultimate decision of the case, the fact that this was considered by the case underscores that the mode of analysis in this factor is one that the Court has weighed before.

209. *See* Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 1005–11 (2013) (offering a survey of techniques for evading surveillance).

210. *See* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 17 (2018).

society.[211] The increasingly comprehensive reach of new technologies arguably raises the costs of this growing arms race, as people wishing not to be subject to surveillance must adjust their conduct with respect to an ever-growing range of behavior. These losses are different from how lack of options abrogates any claim that the defendant voluntarily assumed the risk of disclosing certain information.[212] That concern focuses on individual fairness, while this concern centers on how foregoing certain activities or taking steps to avoid detection can reduce social welfare if the costs of those measures exceed the benefits.

The social costs of this foregone behavior are not confined to economic losses. As Justice Marshall noted in his dissent in *Smith v. Maryland*,

> Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.[213]

Justice Sotomayor drew a similar conclusion in *Jones*, acknowledging that "[a]wareness that the Government may be watching chills associational and expressive freedoms."[214]

These judicial decisions reflect a greater willingness to take the impact of second-order consequences on social welfare into account when assessing whether a particular law enforcement practice violates the Fourth Amendment.

---

211. *E.g.*, Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623, 633 (2015) (arguing that surveillance can create an "arms race" that is "suboptimal" and ties up "efforts and resources [that] could be spared and redirected elsewhere"); Stephen L. Davis, *Conflicting Court Decisions Leave Constitutional Privacy Protections Against Mass Data Collection Uncertain*, J. INTERNET L., May 2014, at 3, 11 (arguing similarly that the government's increasing ability to conduct surveillance will cause computers users to divert "significant resources to conceal information from government's surveillance methods" and that "[w]e may well decide, reasonably, that as a society our resources are better spent elsewhere"); *see also* A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95, 157–58 (2017) ("Counter-surveillance plans and programs such as these serve to remind us that even though at this moment it seems that identification and surveillance have the upper hand, the outcome of this arms race is never certain except in one way: the fight will be expensive.").

212. RESTATEMENT (SECOND) OF TORTS, *supra* note 89, § 496E.

213. Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., joined by Brennan, J., dissenting).

214. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

E. The Underlying Values and the Relative Importance of the Factors

An examination of the evidence on which the Court bases its Fourth Amendment decisions provides a useful basis for distinguishing among the different values at stake. Although there is some overlap in the factors, each emphasizes a distinctly different primary value.

For example, the Law Enforcement Conduct factor's focus on the behavior of government officials reveals that its primary concern is curbing abusive conduct by the state. At the same time, because it does not directly consider the conduct of the defendant in revealing the information, the relative importance of that information, or the impact on broader society, it does not implicate the other values of fairness to the defendant, protection of defendants' substantive privacy interests, or aggregate social welfare. Similarly, the Defendant Conduct factor does not concentrate on the conduct of the government (and whether it might be abusive), the sensitivity of the information (and whether it might implicate defendants' substantive privacy values), or the societal impact (and the net impact of surveillance on aggregate social welfare). The Information Sensitivity factor is the only one that considers defendants' substantive privacy interests directly and ignores how the government obtained that information or how the defendant might have revealed it. The Societal Impact factor is distinctive in that it extends beyond the interests of defendants and law enforcement directly implicated by the surveillance and instead emphasizes the interests of society as a whole.

Our evidence-based approach also reveals how these values have changed over time. For example, the Law Enforcement Conduct factor represented the focus on the Supreme Court's seminal decision in *Boyd* and was repeatedly emphasized in Fourth Amendment decisions during the Rights Revolution period of the 1950s through the 1970s, only to drop off thereafter before playing more prominent roles in *Jones* and *Carpenter*.[215] Similarly, the Court repeatedly raised concern about the dragnet-type practices mentioned in *Knotts* through 1973,[216] only to stop mentioning it again until *Jones* and *Carpenter*.[217] This suggests that this concern faded for a time but is making a revival prompted by the emergence of technologies that make comprehensive surveillance easier to undertake.

---

215. *Id.* at 409 n.6 (majority opinion); Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018); *id.* at 2239–40 (Thomas, J., dissenting); *id.* at 2251 (Alito, J., joined by Thomas, J., dissenting); *id.* at 2264 (Gorsuch, J., dissenting).

216. *See* Cupp v. Murphy, 412 U.S. 291, 294 (1973); United States v. Dionisio, 410 U.S. 1, 11 (1973).

217. *Jones*, 565 U.S. at 409 n.6; *Carpenter*, 138 S. Ct. at 2215 n.2; *id.* at 2230–32 (Kennedy, J., joined by Thomas & Alito, JJ., dissenting).

Emphasis on the Defendant Conduct factor has faded in recent decades. In *Kyllo*, the Court declined to follow the formalistic reasoning of the court below that simply looked at whether heat emanated from a home was visible from the street in favor of an analysis that reflects concern for defendants' expectations in light of changing technology.[218] Similarly, the *Carpenter* Court rejected the straightforward application of the third-party doctrine followed by the court below in favor of a new approach that balanced the fact that the defendant had revealed the information in question against the sensitivity of the information revealed.

At the same time, the Information Sensitivity factor has played a sharply enhanced role over the past two decades. This is apparent in *Kyllo*'s embrace of the home as a proxy for intimate activity and the concern in *Jones* and *Carpenter* for comprehensive tracking of movements. It culminated in the direct analysis in *Riley v. California* and *Carpenter* of the nature of the information potentially seized.

Finally, the Societal Impact factor represents a nascent dimension in the Supreme Court's Fourth Amendment jurisprudence. Focus on the second-order effects of broader surveillance represented prominent features in the dissents in *Smith v. Maryland* and *Jones*. In terms of the direct effects on law enforcement, we suspect that enhanced surveillance's potential to help solve otherwise insoluble crimes will play an increasing role in Fourth Amendment analysis.

Our analysis also reveals a distinctive shift in the Court's Fourth Amendment jurisprudence. Reminiscent of the familiar distinction between formal and substantive approaches to adjudication,[219] Richard Fallon differentiates between *ascriptive* and *descriptive* rights.[220] Ascriptive rights are entitlements that are ascribed to people by virtue of the fact that they are human beings.[221] Because they are deontological, ascriptive rights are necessarily possessed to the same degree by every person.[222] Descriptive rights refer to a person's ability to meaningfully exercise an entitlement.[223] Descriptive rights are empirical and refer to a status that is sometimes attained by different people at different times to varying degrees.[224]

---

218. United States v. Kyllo, 190 F.3d 1041, 1046 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).

219. See Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1686 (1976), for the classic statement.

220. See Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 877 (1994), for the seminal statement of this dichotomy. See Jessica Wilen Berg, *Understanding Waiver*, 40 HOUS. L. REV. 281, 336 (2003), for an application of these principles to the Fourth Amendment.

221. Fallon, *supra* note 220, at 878.

222. *Id.* at 890–91.

223. *Id.* at 877–78.

224. *Id.* at 879–80.

The Court has rejected trespass as the sole touchstone of the Fourth Amendment and no longer treats the revelation of information to third parties as dispositive. We view these holdings as reflecting a shift away from an ascriptive vision of Fourth Amendment rights. At the same time, the greater willingness to engage in a more functional analysis that considers the pervasiveness of the surveillance, the amount of private information revealed in open fields, the reasonableness of any inferences of consent, and the sensitivity of the information obtained reflects an embrace of a more descriptive approach to the constitutionality of surveillance.

II. EMERGING BIOMETRIC TECHNOLOGIES

To illustrate the framework outlined in Part I in practice, this Part considers law enforcement use of three biometric technologies: facial recognition technology (FRT), iris recognition technology (IRT), and DNA profiling. Law enforcement can use these technologies in a variety of ways that might raise Fourth Amendment concerns—from searches with individualized suspicion and the voluntary cooperation of defendants to dragnet, suspicionless surveillance of a community. The variation in how law enforcement can use these technologies provides an opportunity to see how our framework can highlight which Fourth Amendment values are at play.

The Supreme Court has only begun to consider the application of the Fourth Amendment to emerging biometric technologies.[225] These cases, however, represent a narrow set of the uses of biometric technologies. In these cases, the defendant typically had notice that law enforcement was collecting evidence and conducting a search.[226] Moreover, the cases to date have only involved the direct use of genetic material, be it blood from a blood draw or breath into a breathalyzer. In contrast, FRT, IRT, and DNA profiling can be used without suspicion, on a large scale, and sometimes without the knowledge of the defendant at all. We believe the application of our framework to the use of these three technologies is instructive in highlighting the framework's explanatory power in revealing what values underlie a Fourth Amendment analysis.

---

225. *See, e.g.*, Missouri v. McNeely, 569 U.S. 141 (2013); Maryland v. King, 569 U.S. 435 (2013); Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602 (1989); Schmerber v. California, 384 U.S. 757 (1966).

226. We do not comment on whether the defendant received *fair* notice about the search in these cases. It is sufficient that the defendant was proximate to the collection of data for our purposes of drawing a comparison between the cases the Court has heard so far and some of the uses of FRT, IRT, and DNA profiling we will discuss.

A. Facial Recognition Technology (FRT)

Facial recognition is the "process of comparing two images of faces to determine whether they represent the same individual."[227] Facial recognition technology (FRT) operates by detecting and normalizing a face in an image, extracting relevant features of the face, and determining how similar the face in the image is to one or more other faces.[228] There are two common uses of FRT. *Facial verification* determines whether two faces represent the same individual (one-to-one matching).[229] For example, the use of a face as a form of two-factor authentication when performing functions such as unlocking a phone is a form of facial verification.[230] *Facial identification* determines if a given facial image matches any individuals in a set of images with sufficiently high confidence (one-to-many matching).[231] Facial identification can, in turn, take one of two forms. First, law enforcement can check an image of an *unknown* individual against a database of images of *known* individuals, as is done when checking a person's face against a library of mugshots in an attempt to identify her.[232] Second, they can check an image of a *known* person against a database of *unknown* individuals, for example, by using surveillance footage to try to determine the location of a suspect.[233] FRT can also be divided into *cooperative* and *noncooperative* scenarios, depending on users' awareness of the use of facial recognition and their willingness to present their faces consistently and clearly.[234]

In the law enforcement context, uses of FRT also vary based on the level of individualized suspicion possessed by law enforcement before its use. For example, FRT can be used to screen for a single individual for whom there is probable cause to believe has committed a crime. FRT can also be used in a less targeted manner, such as when local, state, and federal law enforcement officials indiscriminately subjected all 100,000 people attending the 2001 Super Bowl to FRT.[235]

---

227. CLARE GARVIE ET AL., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 9 (2016), https://perma.cc/ER8U-C3AP.

228. Stan Z. Li & Anil K. Jain, *Introduction* to HANDBOOK OF FACE RECOGNITION 1, 4 (Stan Z. Li & Anil K. Jain eds., 2011).

229. *Id.* at 2–3.

230. Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRONICS & ROBOTICS 237, 242 (2019).

231. Li & Jain, *supra* note 228, at 3.

232. *See* Andrew G. Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1112 (2021) (calling this practice "face identification").

233. *See id.* at 1113 (calling this practice "face tracking").

234. Li & Jain, *supra* note 228, at 3.

235. *Biometrics Used to Detect Criminals at Super Bowl*, ABC NEWS (Feb. 13, 2001), https://perma.cc/GGA3-EV5E. FRT detected nineteen petty criminals, and because the program was just a test, none were arrested. Susan McCoy, *O' Big*

If the images also contain location metadata, FRT can be used to aggregate the location of the individual through the matching images.

While FRT can make searching through noisy image data more efficient, it is not without serious limitations. FRT performs best with cooperative subjects, and FRT with uncooperative subjects remains an area of continued research and development.[236] Moreover, recent research has highlighted that current FRT exhibits significant racial disparities. In a 2018 study, all tested commercial FRT "performed best for lighter individuals and males" and "worst for darker females."[237] A subsequent study by the National Institute of Standards and Technology of commercial FRT's performance on domestic law enforcement images found high false positive rates for American Indians, African Americans, and Asians, with rates varying between ten and one hundred times depending on the precise demographic in question.[238] Three high-profile examples where FRT misidentification led to the arrest of three innocent African American men have led to lawsuits challenging FRT as impermissibly biased.[239]

In recent years, cities and states have passed legislation to curb the use of facial recognition. San Francisco, Boston, Los Angeles, and

---

Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology, 20 J. MARSHALL J. COMPUT. & INFO. L. 471, 476 n.29 (2002). Cities have long used similar practices in lower profile situations. *See, e.g.*, Michael J. Gerhardt, *The Rhetoric of Judicial Critique: From Judicial Restraint to the Virtual Bill of Rights*, 10 WM. & MARY BILL RTS. J. 585, 640 n.278 (2002) (citing the use of FRT on images obtained from hidden cameras in Times Square, commuter trains in the San Francisco Bay area, rural Mississippi school districts, and downtown Tampa).

236. Frederick W. Wheeler et al., *Face Recognition at a Distance*, *in* HANDBOOK OF FACE RECOGNITION, *supra* note 228, at 353.

237. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 12 (2018).

238. PATRICK GROTHER ET AL., U.S. DEP'T OF COM., NISTIR 8280, FACE RECOGNITION VENDOR TEST (FRVT), PART 3: DEMOGRAPHIC EFFECTS 2, 7 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. The study found higher false negative rates for Asians and American Indians. *Id.* at 3, 7.

239. Drew Harwell, *Wrongfully Arrested Man Sues Detroit Police over False Facial Recognition Match*, WASH. POST (Apr. 13, 2021), https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/ (reporting that Williams has also filed a lawsuit); Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html (reporting the cases of Nijeer Parks, Robert Williams, and Michael Oliver, and noting that Parks and Oliver have filed lawsuits); *see also* Bah v. Apple, Inc., No. 19-cv-3539, 2021 WL 4084500, at *9–10 (S.D.N.Y. Sept. 8, 2021) (dismissing a § 1983 claim based on law enforcement officials' misuse of FRT because the arrest was based on a superficially valid warrant).

Portland have all banned facial recognition in their cities.[240] New York has banned the use of FRT (as well as other biometric technology) in schools.[241] Illinois passed the Biometric Information Privacy Act to regulate the storage and collection of biometric data, which includes data for facial recognition.[242] Despite this growing movement to ban or place a moratorium on FRT, federal law enforcement and law enforcement in areas without local regulation can still use FRT.

1. The Law Enforcement Conduct Factor (Factor 1)

Law enforcement can use FRT in a variety of ways when conducting a search. Law enforcement may use FRT for facial verification during a police booking procedure. It may also apply FRT to video feeds and images scraped from social media to engage in facial identification or to track an individual's movements, creating a "newfound tracking capacity [that] runs against everyone" similar to the use of CSLI in *Carpenter*.[243]

The propriety of the government's conduct depends in large part on how the image used in FRT is collected. For example, the companion cases of *Ciraolo* and *Dow Chemical* established the constitutionality of using cameras to collect images for public locations.[244] Images obtained from driver's license photos are not likely to raise concerns in this regard.[245] *Carpenter* also recognized in dicta that its holding did not "call into question conventional surveillance techniques and tools, such as security cameras,"[246] and subsequent courts have held that *Carpenter* did not displace the long-established principle that images taken by cameras in public places do not constitute searches.[247]

In addition to the fact-specific analysis of the search's location, we can examine whether law enforcement conduct has the characteristics of dragnet surveillance. Limited use of FRT, such as to determine whether a person in custody might be wanted for other

240. Press Release, Am. Civ. Liberties Union, Portland City Council Unanimously Passes Face Surveillance Ban, but Without Important Enforcement Provisions (Aug. 4, 2020), https://perma.cc/BJ7B-ABWR; Rebecca Klar, *Los Angeles Police Ban Use of Third-Party Facial Recognition Software*, HILL (Nov. 18, 2020), https://thehill.com/policy/technology/526487-los-angeles-police-ban-use-of-third-party-facial-recognition-software.

241. N.Y. STATE TECH. LAW § 106-b (2024).

242. 740 ILL. COMP. STAT. 14/5 (2024).

243. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

244. California v. Ciraolo, 476 U.S. 207, 213, 215 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

245. *See, e.g.*, Hill, *supra* note 239.

246. *Carpenter*, 138 S. Ct. at 2220.

247. *See, e.g.*, United States v. Tuggle, 4 F.4th 505, 514–16 (7th Cir. 2021); United States v. Moore-Bush, 963 F.3d 29, 39–42 (1st Cir. 2020).

crimes, is unlikely to be regarded as overreaching under this factor. FRT, however, can also provide law enforcement with the ability to efficiently perform arbitrary or suspicionless surveillance, such as the one that occurred at the 2001 Super Bowl, in which law enforcement applied FRT to a group of people without a specific suspect or specific crime in mind. Such use of FRT permits the type of retrospective reconstruction that raised concerns in *Carpenter*.[248]

Applying FRT to datasets that combine image and location data would also permit law enforcement to build the type of comprehensive log of a person's movements decried by the *Carpenter* majority and five Justices in *Jones*.[249] If law enforcement used FRT in this manner, this factor would motivate the determination that the search was unreasonable. Courts have recognized that the use of cameras that "captured only a small slice of the daily lives of any residents, and then only when they were in particular locations outside and in full view of the public" does not raise the type of "comprehensively invasive" law enforcement use that *Carpenter* held unconstitutional.[250] At the same time, placing "enough cameras in enough locations" would "allow the police to reconstruct people's past movements without knowing in advance who police are looking for" and could create a sufficiently "substantial picture of the defendant's public movements" to run afoul of *Carpenter*.[251]

As such, we can use the comprehensiveness of the tracking that law enforcement performs with FRT as an empirical, evidentiary standard to gauge whether society would accept that use of FRT as reasonable.

2. The Defendant Conduct Factor (Factor 2)

a. Exposure by the Defendant

Image data for FRT can come from a variety of sources, but three common categories of data sources are specifically important for a Fourth Amendment analysis: (1) images directly provided to law enforcement by that defendant, (2) images taken in public or shared spaces, and (3) images taken by a third party. At one extreme, defendants may knowingly provide their photographs to the government for the purpose of identification. At the other, defendants

248. *Carpenter*, 138 S. Ct. at 2218.

249. *See supra* notes 51, 53, 56 and accompanying text.

250. *See Moore-Bush*, 963 F.3d at 42; *accord Tuggle*, 4 F.4th at 525–26 (holding that the use of three cameras mounted on utility poles did not create the type of comprehensive and retrospective record of a the defendant's movements found problematic in *Carpenter*); Commonwealth v. McCarthy, 142 N.E.3d 1090, 1106 (Mass. 2020) (holding that the use of four cameras monitoring access to an island across two bridges did not track enough of defendant's public movements to fall within *Carpenter*).

251. *McCarthy*, 142 N.E.3d at 1104.

may not know that they are the subject of an image, let alone an image that will later be subject to FRT.

First, when defendants provide images directly to law enforcement through driver's license photos, mugshots, or visa applications, they typically have ample notice of the possibility that law enforcement will use the image for identification. For example, the FBI's Next Generation Identification Interstate Photo System (NGI-IPS), its facial recognition database, contains 25 million state and federal criminal photos.[252] The FBI's Facial Analysis, Comparison, and Evaluation (FACE) Services unit uses a network of federal and state databases that contains driver's license photos from twelve states and both driver's license photos and mugshots from another four states.[253] Both mugshots and driver's license images are taken, at least in part, for government identification.

Second, in the case of images taken in public or shared spaces, the Court has recognized that people who knowingly expose their faces in public have assumed some risk of identification.[254] Although *Carpenter* introduced additional considerations that must be taken into account,[255] in so doing, it underscored that this new framework was not meant to call into question the constitutionality of using security cameras.[256] Post-*Carpenter* decisions by lower courts have reaffirmed that the analysis is the same regardless of whether the camera is operated by a private actor or by the government.[257]

Third, any images used for FRT that the defendant voluntarily shared with third parties may enjoy reduced expectations of privacy, barring any contractual obligations that prevent warrantless access to the third-party data. Although *Carpenter* made clear that sharing data with third parties is not by itself dispositive, its reasoning and the fact that it adhered to the holdings in *Smith* and *Miller* reveal that sharing data with third parties remains an important consideration.[258]

b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant

Under our framework, the legal significance of any exposure of images by the defendant depends on what risks courts may regard the defendant as having voluntarily undertaken by doing so. When making this determination, courts have considered whether a

252. GARVIE ET AL., *supra* note 227, at 13.

253. *Id.*

254. *See supra* notes 29, 58–64, 85–87 and accompanying text.

255. *See supra* notes 95–96, 129–32 and accompanying text.

256. *See supra* note 246 and accompanying text.

257. *See, e.g.*, United States v. Moore-Bush, 963 F.3d 29, 40 n.11 (1st Cir. 2020).

258. *See supra* notes 98–99 and accompanying text.

technology is generally available and whether it is generally or routinely used by the public.[259]

To evaluate the conduct of the defendant, we must thus ask whether FRT is in sufficiently widespread use to justify regarding potential defendants' exposure of their images to the public a voluntary assumption of the risk of being subjected to FRT.

Much like with image data collected in shared or public spaces, we might also accept an expectation of privacy from tracking one's movements in image data given to a third party. The use of image-sharing platforms, social media, or cloud storage has become more commonplace, even though individuals might find the metadata collection and regular camera use threatening to individual privacy.[260] The Court has highlighted that the defendant's conduct alone, as governed by the third-party doctrine, is not dispositive; while it is reasonable for a defendant to assume the risk in sharing small amounts of data, it becomes more unreasonable to expect that defendants assume the risk in sharing large amounts of data, especially when the scope of data approaches a "comprehensive dossier" as described in *Carpenter*.[261] As the use of location metadata from third-party images becomes more routine, courts may view the extension of the third-party doctrine to larger amounts of data as more reasonable. So far, however, the Court has held that the third-party doctrine cannot mechanically apply to situations that force the defendant to assume the risk for their entire movements.[262]

The proliferation of cameras in our modern society, including traffic cameras, closed circuit television (CCTV), or cell phone cameras, makes it increasingly likely that courts will view defendants' decisions to expose their faces in public as a voluntary assumption of the risk of being subjected to FRT. Image data from public or shared sources has become ubiquitous, and the use of image data from a third party for identification sources is likely analogous. More often than ever before, people share, upload, post, and send images online. In fact, FRT for identification is already commonplace

---

259. *See supra* notes 110, 114, 118–19 and accompanying text.

260. In fact, the Court has recognized this trade-off that individuals make between increased convenience and decreased privacy. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., joined by Ginsburg, Breyer & Kagan, JJ., concurring in the judgment) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

261. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

262. *Id.* at 2219 ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

in non-law enforcement contexts.[263] While FRT was still nascent a decade ago, these commonplace uses of FRT, coupled with the amount of image data that pervades our modern society, make it a matter of time before FRT reaches the point where anyone appearing in public is on notice that their image may be captured and subjected to FRT if that point has not been reached already.

3. The Information Sensitivity Factor (Factor 3)

Following *Carpenter*, courts must, of course, balance the fact that a defendant may have voluntarily subjected their images to FRT against the sensitivity of the information revealed.[264] In this regard, we consider two distinct practices: first, the comparison of an individual face against other faces in a database of images, and second, the combination of the image analysis with location metadata about where the image was taken.

Regarding the use of image data, in theory, we have some privacy interest in what our face can reveal. Faces can reveal age, sex, and race, and sometimes even details about one's cultural practices or personal health. All of these characteristics implicate significant privacy interests. Furthermore, images often contain other faces that can reveal friends, relatives, or business associates of defendants. This additional information can reveal information about the defendant's associations, which might merit a stronger privacy interest than that which we place on just images of our faces.[265] By determining who we are seen with in photos or videos, especially in aggregate, law enforcement can use FRT to understand information about our patterns of life that would not otherwise be easily ascertainable.

In practice, arguments about the sensitivity of information revealed from people's faces have largely been foreclosed by the Court's explicit recognition that its decision in *Carpenter* did not "call into question conventional surveillance techniques and tools, *such as security cameras*."[266] This categorical holding essentially rules out arguments that the facial images obtained by security cameras reveal information that is so sensitive as to render the practice unconstitutional on those grounds alone.

Linking facial images with location metadata is potentially more problematic. On the one hand, courts are unlikely to raise many

263. While facial verification and identification are not the same workflow, the underlying technology remains the same. The software uses a facial recognition model to perform a 1:1 match in facial verification and a 1:N match in facial identification. *See, e.g.*, *About Face ID Advanced Technology*, APPLE (Jan. 10, 2024), https://perma.cc/Q3V2-H4MV; *Unlock Your Pixel Phone with Your Face*, GOOGLE (2024), https://perma.cc/ZZU2-3U8C.

264. *See supra* notes 185–87 and accompanying text.

265. *See supra* notes 172–73, 185 and accompanying text.

266. *Carpenter*, 138 S. Ct. at 2220 (emphasis added).

concerns about combining images with a single piece or a limited amount of location information. On the other hand, the proliferation of cameras and stored images that put the defendant on notice of the risk of being subjected to FRT also increases the amount of location information that can be correlated with a particular image. Combining images with larger amounts of location data can provide the type of comprehensive and retrospective record of a person's movements that concerned members of the Court in *Knotts* and *Jones* and that the Court found problematic in *Carpenter*.[267] To the extent that it can be correlated with the location of others, it can also reveal information about a person's associations and affiliations that the Court may consider private.[268]

Lower courts have adhered to this standard as well in evaluating the defendant's expectation of privacy in similar cases. For example, in *Commonwealth v. McCarthy*,[269] the Massachusetts Supreme Judicial Court recognized that the collection of information from too many locations could provide the type of comprehensive location information that raises constitutional concerns but concluded that the limited amount of location information collected by four cameras at the ends of two bridges did not reach that level.[270] Similarly, in *United States v. Moore-Bush*,[271] the First Circuit rejected arguments that the installation of a camera on a utility pole in front of the defendant's house violated the Fourth Amendment, holding that the pole cameras "captured only a small slice of the daily lives of any residents, and then only when they were in particular locations outside and in full view of the public."[272] In fact, these cameras "captured *less* information about [the defendants] than someone on the street could have seen and captured."[273]

Thus, whether FRT implicates the Information Sensitivity factor depends on the amount of location information that it yields. Although there have yet to be cases brought against law enforcement for using FRT to track people's movements, courts assessing the constitutionality of the practice would have to assess the comprehensiveness of that information.

4. The Societal Impact Factor (Factor 4)

This last factor of analysis considers the first- and second-order implications of encouraging the use of FRT in society. As a first-order result, we might see more law enforcement use of this technology to

267. *See supra* notes 159–60, 143–45 and accompanying text. For a similar argument, see Ohm, *supra* note 13, at 366.

268. *See supra* notes 172–73, 185 and accompanying text.

269. 142 N.E.3d 1090 (Mass. 2020).

270. *Id.* at 1104–06.

271. 963 F.3d 29 (1st Cir. 2020).

272. *Id.* at 42.

273. *Id.*

investigate crimes. As a second-order result, we need to consider the broader implications on society from an increased use of FRT in investigating crimes.

a. The Social Benefits of More Effective Law Enforcement (Factor 4A)

In certain instances, FRT has helped law enforcement identify uncooperative suspects. For example, on June 28, 2018, a gunman fatally shot five employees of the *Capital Gazette*, a newspaper serving Annapolis, MD, at the newspaper's headquarters. Once arrested, officers were able to identify the suspect with the help of facial recognition technology because the suspect did not have identification on him and was not cooperative.[274] Once the police were able to identify the subject, they discovered a previous feud between the suspect and the *Capital Gazette*.[275] In this case, FRT was an efficient and nonintrusive means of identifying a suspect and determining a potential motive. Notably, in this case, law enforcement had individualized suspicion and used FRT at the police station after the suspect was apprehended, which obviated many of the privacy risks associated with suspicionless or arbitrary surveillance.[276]

FRT could also be used for lead generation if law enforcement is presented with an unknown face to identify. This approach, however, is not without significant risks. A 2020 NIST review found that one-to-many facial recognition algorithm accuracy varied significantly based on the FRT vendor, with false negative rates ranging from less than 1% to over 50%.[277] In fact, the biases of FRT software may prevent law enforcement from finding accurate leads. Commercial facial recognition algorithms vary significantly in their false positive

274. *See generally* Justin Jouvenal, *Police Used Facial-Recognition Software to Identify Suspect in Newspaper Shooting*, WASH. POST (June 29, 2018), https://www.washingtonpost.com/local/public-safety/police-used-facial-recognition-software-to-identify-suspect-in-newspaper-shooting/2018/06/29/6dc9d212-7bba-11e8-aeee-4d04c8ac6158_story.html; Ian Duncan & Luke Broadwater, *Suspect Swore 'Oath' to Kill Capital Staff Years Ago, Had Restraining Orders—But Bought Gun Legally*, CHI. TRIB. (Aug. 21, 2019), https://perma.cc/D2WN-2Y72.

275. Duncan & Broadwater, *supra* note 274.

276. See *supra* Section II.A.1 for an analysis of law enforcement when using FRT.

277. PATRICK GROTHER ET AL., U.S. DEP'T OF COM., NISTIR 8271, FACE RECOGNITION VENDOR TEST (FRVT), PART 2: IDENTIFICATION 7 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf ("Recognition accuracy is very strongly dependent on the algorithm and, more generally, on the developer of the algorithm. False negative error rates in a particular scenario range from a few tenths of one percent to beyond fifty percent.").

rates across gender and racial groups.[278] Moreover, police departments themselves have released statements cautioning about the use of FRT for generating leads, especially without individualized suspicion.[279]

In addition, identifying suspects with FRT in practice may not be as helpful as imagined. Only a very small sample of images may serve as possible leads,[280] and the failure modes of FRT can lead to wrongful arrests. For example, in January 2020, the Detroit Police Department wrongly arrested Robert Williams as a suspect in a retail fraud case with a lead based on FRT.[281] While improvements in the accuracy, bias, and oversight of FRT may eventually make it more effective, the current use of FRT for lead generation may be limited.

With the current generation of FRT, there may not be many cases in which FRT is both necessary and sufficient for solving an investigation. If other approaches do not present the same risks as FRT that law enforcement could sufficiently use instead, then courts would be less likely to forgive the warrantless use of FRT, even if it is effective in that one instance. This factor of the analysis considers not only whether the technology is accurate and efficient but also whether the use of technology balances the needs of society with the potential risks of the technology. If future developments improve FRT with respect to these performance, bias, and ethical concerns, then the new empirical and contextual considerations could motivate the outcome of this factor.

b. The Social Costs of Avoidance Behavior (Factor 4B)

As noted above, an assessment of the social impact requires assessing the costs as well as the benefits of authorizing a particular form of law enforcement surveillance. In particular, courts may consider the second-order consequences of allowing broader use of FRT.

For example, those wishing to avoid having their facial images captured on cameras may become more hesitant to exercise their rights of expression and association.[282] Those wishing to frustrate FRT may also use masks to increase the false match rate of some

278. Buolamwini & Gebru, *supra* note 237, at 12; GROTHER ET AL., *supra* note 238, at 2.

279. Kevin Rector & Richard Winton, *Despite Past Denials, LAPD Has Used Facial Recognition Software 30,000 Times in Last Decade, Records Show*, L.A. TIMES (Sept. 21, 2020), https://www.latimes.com/california/story/2020-09-21/lapd-controversial-facial-recognition-software.

280. GARVIE ET AL., *supra* note 227, at 26 ("Of the FBI's 36,420 searches of state license photo and mug shot databases, only 210 (0.6%) yielded likely candidates for further investigations.").

281. Harwell, *supra* note 239.

282. Commonwealth v. McCarthy, 142 N.E.3d 1090, 1104–05 (Mass. 2020).

facial recognition algorithms and models,[283] though FRT developers have, in turn, countered this evasion technique with new periocular facial recognition algorithms.[284] Even more elaborate methods to prevent facial recognition include lasers, infrared light, or clothing with patterns that intentionally cause false negatives.[285] Such methods to avoid facial recognition, however, cannot be so burdensome that they would become impractical or themselves constitute a distortion to societal behavior.[286]

5. Summation

Each use of FRT invites a unique value-based analysis to elucidate what aspects of the technology drive the belief that an FRT-enabled search is or is not reasonable. For FRT identification workflows, the question of reasonableness is rooted in the Information Sensitivity factor (Factor 3) and the risk of ethical malfeasance that undercuts the potential benefit to efficient law enforcement (Factor 4). For FRT tracking workflows, the unreasonableness of such searches stems from the dragnet surveillance conduct of law enforcement (Factor 1) and the heightened expectation of privacy of the defendant due to the use of novel, non-routine technology (Factor 2). If location data is aggregated and analyzed as part of this tracking as well, the aggregation of location information begs concerns about revealing sensitive information (Factor 3) and chilling democratic liberties, even though it might make law enforcement more efficient (Factor 4).

B. Iris Recognition Technology

Popularized by the movie *Minority Report*, Iris Recognition Technology (IRT) identifies individuals by comparing their iris patterns to those of known individuals.[287] In iris recognition, the iris

283. MEI NGAN ET AL., U.S. DEP'T OF COM., NISTIR 8311, ONGOING FACE RECOGNITION VENDOR TEST (FRVT), PART 6A: FACE RECOGNITION ACCURACY WITH MASKS USING PRE-COVID-19 ALGORITHMS, at ii (2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf.

284. MEI NGAN ET AL., U.S. DEP'T OF COM., NISTIR 8311, ONGOING FACE RECOGNITION VENDOR TEST (FRVT), PART 6B: FACE RECOGNITION ACCURACY WITH FACE MASKS USING POST-COVID-19 ALGORITHMS, at i (2022), https://pages.nist.gov/frvt/reports/facemask/frvt_facemask_report.pdf ("[T]he results show evidence that a number of developers have adapted their algorithms to support face recognition on subjects potentially wearing face masks.").

285. Mara Hvistendahl & Sam Biddle, *Homeland Security Worries Covid-19 Masks Are Breaking Facial Recognition, Leaked Document Shows*, INTERCEPT (July 16, 2020), https://perma.cc/KPW2-G2EH.

286. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986) (addressing the idea that Dow should have to shield its manufacturing plant from overhead view, to which the Court noted that "it could hardly be expected that Dow would erect a huge cover over a 2,000-acre tract")

287. MINORITY REPORT (20th Century Studios & DreamWorks Pictures 2002).

is encoded into a set of features—an "iriscode"—either through an algorithm specifically designed for iris feature encoding or a trained model.[288] Analogous to FRT, the iriscode generated from the image of the unknown iris is then compared against the iriscodes of known individuals to find high-confidence matches. The iris contains many distinctive features, but only some of these features can be easily seen in visible light. Near-infrared (NIR) light can be used to better visualize the complex structure of the iris, especially the structure of internal layers.[289]

While IRT and FRT share a common technical approach, there are key differences between the two technologies that impact the application of our framework. First, IRT often requires specific sensors, as iris recognition is usually performed in the NIR spectrum of light.[290] Second, IRT does not perform well over large distances. Typically, the individual must be within a few feet of the IRT sensor.[291] These technical restrictions limit the use of IRT in noncooperative settings and will impact all four factors because they prevent some of the covert surveillance workflows that FRT could enable. Long-range iris recognition—or Iris at a Distance (IAAD) technology—is a current area of research, and some applications of long-range iris recognition have already been commercialized for use in walkthrough or drivethrough portals.[292] FRT, however, will likely outperform IRT at long distances.[293]

---

288. John Daugman, *How Iris Recognition Works*, 14 IEEE TRANSACTIONS ON CIRS. & SYS. FOR VIDEO TECH. 1, 21 (2004). Daugman pioneered the work for creating iriscodes. Now, machine learning approaches can create efficient iriscodes as well. Kien Nguyen et al., *Iris Recognition with Off-the-Shelf CNN Features: A Deep Learning Perspective*, 6 IEEE ACCESS 18848, 18848 (2018).

289. Daugman, *supra* note 288, at 21–22.

290. GEORGE W. QUINN ET AL., U.S. DEP'T OF COM., NISTIR 8252, IREX IX PART TWO: MULTISPECTRAL IRIS RECOGNITION 12 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8252.pdf ("All currently deployed iris recognition systems operate on iris images illuminated in the near infrared (NIR) band of the electromagnetic spectrum . . . . NIR light is specified because melanin, the pigment that makes dark eyes dark, is nearly transparent in the NIR. This makes the stromal structure of dark brown irises easier to resolve.").

291. Kien Nguyen et al., *Long Range Iris Recognition: A Survey*, 72 PATTERN RECOGNITION 123, 127 (2017) ("Compared to face, iris recognition systems require the user to be in close range to the sensor (i.e., less than 1 m). It has to be noted that the acquisition distance is often referred as the *stand-off* distance (distance between the user and sensor).").

292. *Id.* at 129 ("The original IOM product is available on the market with two application-specific versions: walk-through portal . . . and drive-through portal.").

293. Wheeler et al., *supra* note 236 ("For security or covert applications, facial imaging can be achieved without the knowledge of the subject. There is great interest in iris at a distance, however it is doubtful that iris will outperform face with comparable system complexity and cost.").

At the same time, IRT is much more accurate than FRT. In a 2018 NIST review, the best one-to-many iris recognition algorithm had a 1-in-1000 false positive match rate and a 1-in-150 false negative match rate.[294] These low false positive and false negative rates make iris recognition a likely biometric technology for law enforcement adoption.[295]

1. The Law Enforcement Conduct Factor (Factor 1)

The current technical limitations of IRT will likely deter law enforcement from using the technology in a manner that raises Fourth Amendment concerns. For example, it would be impractical for law enforcement to use IRT for dragnet surveillance or without individualized suspicion. Law enforcement can still use IRT to surveil the defendant if it can easily capture images of the defendant's iris and have a database of iriscodes. As of now, IRT offers law enforcement information similar to that from fingerprints: They are taken in controlled settings and usually for the purpose of identification. It would be hard to aggregate a meaningful record of someone's movements with IRT from just these snapshots.

Categorical concerns about law enforcement conduct with IRT become more serious as long-range IRT develops. Concerns about surreptitious surveillance with IRT would be heightened if the technology can accurately operate on uncooperative individuals, with more conventional camera equipment, or from further distances. In such cases, the concerns under this factor will begin to approach those under this factor in the case of FRT.

2. The Defendant Conduct Factor (Factor 2)

a. Exposure by the Defendant (Factor 2A)

As with FRT, we can evaluate defendants' role, if any, in exposing the images of their irises to law enforcement. We analyze separately the same three sources of images that we discussed above with respect to FRT: (1) images directly provided to law enforcement by that defendant, (2) images taken in public or shared spaces, and (3) images taken by a third party.[296]

---

294. GEORGE W. QUINN ET AL., U.S. DEP'T OF COM., NISTIR 8207, IREX IX PART ONE: PERFORMANCE OF IRIS RECOGNITION ALGORITHMS 1 (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8207.pdf ("The most accurate *one-to-many* matcher yields an FNIR (False Negative Identification Rate) of 0.0067 (about 1 in 150) at an FPIR (False Positive Identification Rate) of 10^{-3} (1 in 1000) when searching against an enrolled population of 160 thousand people.").

295. *See, e.g.*, George Joseph, *The Biometric Frontier*, INTERCEPT (July 8, 2017), https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics/.

296. *See supra* Section II.A.2.a.

First, defendants who provide iris images directly to the government will have a hard time arguing that they were not on notice that law enforcement might use those images for IRT. IRT's low false match rate has led many governments and law enforcement agencies to utilize it in their national biometrics programs. For example, the government of India launched a program to register every citizen with a unique identification number that relied on biometric verification from both fingerprints and iris recognition.[297]

Second, in the case of iris images collected from public or shared spaces, courts are likely to regard defendants as having assumed the risk that some third party may collect such publicly exposed iris images. The reasonableness of this expectation must be viewed in light of the frequency with which IRT is used by the general public, which is the topic of the next Section.

Third, in the case of iris images given to third parties, the third-party doctrine governs the defendant's conduct, also indicating that the defendant assumes the risk of sharing such information with a third party. Although *Carpenter* added additional considerations that must be taken into account, it reaffirmed that whether the defendant has given information to third parties remains an important criterion.[298]

The analysis of defendants' conduct in exposing information about their irises is directly analogous to that of FRT. In both cases, actions taken by defendants that made it possible for others to obtain images through public observation or from third parties militate against unconstitutionality.

b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B)

Despite the growing adoption of iris-based biometrics, the lack of public interaction with iris recognition technology, especially in the United States, undercuts the idea that a court would find that IRT is in general or routine public use. As with FRT, the extent to which courts can validly conclude that defendants have assumed the risk of being subjected to IRT depends on defendants' reasonable apprehensions about the implications of their conduct. We can again consider each of the three common categories of sources of image data that framed our prior analysis.[299]

First, concerning iris data given directly to law enforcement, defendants should be aware that it may be used for IRT. There are not many other uses of iris data, and the defendant would have a hard time credibly arguing that using it for IRT came as a surprise.

---

297. Billy Perrigo, *India Has Been Collecting Eye Scans and Fingerprint Records from Every Citizen. Here's What to Know*, TIME (Sept. 28, 2018), https://time.com/5409604/india-aadhaar-supreme-court/.

298. *See supra* note 98 and accompanying text.

299. *See supra* Sections II.A.2.a, II.B.2.a.

Second, in the case of iris scans collected from public spaces, we might accept as reasonable an expectation of privacy from IRT based on publicly collected iris scans. Commercially available IRT generally has poor performance over long distances or in uncooperative settings, both of which are likely necessary to collect iris scans in public.[300] Moreover, the lack of commonly available NIR sensors reduces the likelihood of a third party holding the iris scan of the unknown individual that law enforcement wants to identify.[301] At this time, it would seem extraordinary—and far from the "routine" standard in *Ciraolo* and reaffirmed in *Kyllo*—if anyone could compile a database of iris scans from peoples' movements in public.[302] Thus, under the current technological capabilities of IRT, defendants are not likely to have fair notice that their iris images may be captured when they are driving on public roads or walking in public.

Long-range iris recognition, however, is not far from a commercial reality; in fact, it is an active area of biometrics research.[303] In 2015, researchers developed the "first effective long-range iris scanner," with the ability to detect and recognize a driver's irises from their glances in their rearview mirrors.[304] As long-range IRT continues to develop, defendants are likely to be on notice that law enforcement may capture their iris images when they are traveling in public spaces, much like the proliferation of commercial air flight eroded the defendant's expectation of privacy in *Ciraolo*, *Dow Chemical*, and *Florida v. Riley*.[305]

Third, the case of iris scans held by third parties presents the most challenging questions under this framework. Private biometrics companies often hold data from law enforcement use of IRT. For example, BI2 Technologies provided the IRT used by both the NYPD and counties along the U.S.-Mexico border.[306] As of 2017, BI2 technologies stated that they had the largest iris recognition database in the nation, with close to a million iris scans.[307]

While many private companies may also hold facial recognition data, private control over iris scans is strikingly different. In the case of facial recognition, the defendant gives photographs to a third party,

---

300. *See* Nguyen et al., *supra* note 291 and accompanying text.

301. *See* QUINN ET AL., *supra* note 290 and accompanying text.

302. *See supra* notes 114, 118–19 and accompanying text.

303. *See* Nguyen et al., *supra* note 291 and accompanying text.

304. Robinson Meyer, *Long-Range Iris Scanning Is Here*, ATLANTIC (May 13, 2015), https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/.

305. California v. Ciraolo, 476 U.S. 207, 215 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986); Florida v. Riley, 488 U.S. 445, 450 (1989).

306. Joseph, *supra* note 295.

307. *Id.* ("To make an identification, BI2's iris recognition program compares an individual's iris against the over 987,000 iris scans held in its private database, which collects images from over 180 law enforcement jurisdictions nationwide. . . . The database is the largest of its kind in North America.").

but because photographs can be used in a variety of applications, the defendant may not expect that the third party—whether it be a cloud storage provider or a social media platform or a website to make custom holiday cards—will necessarily use the data for facial recognition.

The data for iris recognition have limited alternative uses. Indeed, it would be hard to imagine a company like BI2 using this data for anything other than iris recognition. Given the limited other use cases for such images of irises, defendants would more likely expect that third parties with their iris scans could use them for biometric identification than they might expect from that same third party if it had their photographs. Compared to facial recognition or even the exposure of CSLI or GPS data, the defendant has more notice that an iris scan given to a third party may be later used for IRT, drawing this example closer to those in *Smith* and *Miller*.

3. The Information Sensitivity Factor (Factor 3)

We evaluate the importance of image data—for both FRT and IRT—on both the information revealed in the image and any metadata associated with the image. We place low importance on the iris patterns themselves, either in isolation or even in aggregate. The intrinsic information contained in iris patterns is quite similar to fingerprints: Both are used for identification, but the data itself does not evoke a sense of privacy or personal importance. Like fingerprints, iris patterns are less personally sensitive than we might find images of our faces and certainly less sensitive than DNA.

Compared to FRT, the lack of a large corpus of IRT data makes combining it with location metadata less likely to create all-encompassing records of a person's movements. Instead, the images will likely have location data of the more controlled settings where the iris scans are often collected. As long-range iris recognition develops, however, the location data that IRT can reveal will become increasingly more sensitive. With advances in uncooperative iris recognition at a distance, our analysis will begin to resemble Information Sensitivity in the case of FRT as well.[308]

The case of IRT demonstrates how technological evolution can impact the outcome of this factor. Today, society might not accept as reasonable a defendant's expectation of privacy in location data collected through IRT. In a future where long-range IRT becomes a reality, society may begin to accept an expectation of privacy in location data from IRT as reasonable, much like how we found the reasonableness of aggregated location data significantly more concerning in our analysis of this Information Sensitivity factor for FRT above.

---

308. *See supra* notes 291–92, 304 and accompanying text. For the analysis of FRT under the Information Sensitivity factor, see *supra* Section II.A.3.

4. The Societal Impact Factor (Factor 4)

With its current technological and practical tradeoffs, IRT might offer law enforcement a means to confirm an unknown identity more accurately and with a greater emphasis on maintaining individual suspicion than would FRT. The current technical limitations of IRT minimize the probability that widescale use of IRT would induce welfare-reducing second-order effects.

a. The Social Benefits of More Effective Law Enforcement (Factor 4A)

Iris recognition has lower false positive and false negative rates than facial recognition.[309] Moreover, the demographic bias of iris recognition is still an active area of investigation, but current experiments with iris recognition algorithms do not show the same and consistent impact of gender and race bias as with algorithms for facial recognition.[310] The reduced impact of bias, better performance, and less intrusive nature of the technology lead to a stronger case for law enforcement use of IRT compared to FRT.

Such benefits to law enforcement, however, must also be weighed against the lack of large databases for IRT. Without access to data to compare the defendant's iris scans against, coupled with limited means for collecting uncooperative iris scans, the technological limitations of IRT currently might make it an inefficient means for solving crimes.

b. The Social Costs of Avoidance Behavior (Factor 4B)

The practical limitations of IRT also serve as a check on the potential distortions to our behavior in society. With the current scope of IRT—that is, discounting law enforcement use of long-range, non-cooperative iris recognition—it is hard to imagine that defendants will engage in the types of avoidance behavior with respect to IRT

309. *See* QUINN ET AL., *supra* note 294 and accompanying text.

310. *Id.* at 2 ("Sex has a significant impact on accuracy for some matchers, but the effect is not consistent . . . . With respect to race, the matchers tend to perform best on Whites and poorest on Asians. This is not true in all cases and sometimes the differences are negligible . . . . [W]e cannot discount the possibility that any apparent demographic effects are due to confounding factors. Further investigation i[s] necessary before drawing any solid conclusions."); JOHN J. HOWARD ET AL., U.S. DEP'T OF HOMELAND SEC., QUANTIFYING THE EXTENT TO WHICH RACE AND GENDER FEATURES DETERMINE IDENTITY IN COMMERCIAL FACE RECOGNITION ALGORITHMS 5, 10 (2021), https://www.dhs.gov/sites/default/files/publications/21_0922_st_quantifying-commercial-face-recognition-gender-and-race_updated.pdf ("The periocular images used in iris recognition bear features related to demographics and both humans and algorithms can readily identify race and gender from periocular images. Nonetheless, iris recognition algorithms based on iris-codes do not utilize these features in making identity determinations." (citations omitted)).

that they might with FRT, CSLI, or GPS tracking. Specifically, the short standoff distance and cooperative settings that IRT requires significantly lessen any concerns of constant, covert, and suspicionless surveillance by law enforcement.

In addition, individuals could disrupt law enforcement's use of long-range IRT in public view as it becomes more commercially available. Contact lenses, eyeglasses, sunglasses, and even certain health conditions of the eye can prevent IRT from making a successful match.[311] While a *de minimis* distortion on society may still be an adverse impact of the technology, the nonintrusiveness and ease of such solutions to disrupt IRT show that the impact of law enforcement's use of IRT on society could be moderated.

5. Summation

This analysis reveals that the motivations for requiring a warrant for iris recognition are different than those for facial recognition. In the case of using IRT for identification, courts would likely attribute the potential unreasonableness of such a search primarily to the reasonableness of inferences drawn from the conduct of the defendant (Factor 2B) and the (in)effectiveness of law enforcement (Factor 4A). If law enforcement also sought to use IRT to aggregate the defendant's movements, the conduct of law enforcement (Factor 1), as well as the potential second-order distortions to society, more significantly represent our underlying values (Factor 4B). The proliferation of long-range IRT would push this analysis to resemble more closely that of FRT.

C. DNA Profiling

As the Supreme Court has noted, "[t]he advent of DNA technology is one of the most significant scientific advancements of our era."[312] In short, "[m]odern DNA testing can provide powerful new evidence unlike anything known before"[313] that makes it "possible to determine whether a biological tissue matches a suspect with near certainty,"[314] which gives "DNA testing . . . an unparalleled ability both to exonerate the wrongly convicted and to identify the guilty" and "has the potential to significantly improve both the criminal

311. QUINN ET AL., *supra* note 294, at 47 ("The remaining 36 comparisons that were not removed generally involve extremely poor quality iris samples (closed eyes, patterned contact lenses, etc.)."); Daugman, *supra* note 288, at 23 ("[I]ris region[s] . . . obscured by eyelids [or] contain[ing] any eyelash occlusions, specular reflections, boundary artifacts of hard contact lenses, or poor signal-to-noise ratio (SNR) . . . should be ignored . . . as artifact[s].").

312. Maryland v. King, 569 U.S. 435, 442 (2013).

313. Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 62 (2009).

314. *Id.*

justice system and police investigative practices."[315] As such, "DNA identification represents an important advance in the techniques used by law enforcement to serve legitimate police concerns."[316] At the same time, DNA-based evidence can be outweighed by other evidence and alternative explanations for the result. "The dilemma is how to harness DNA's power to prove innocence without unnecessarily overthrowing the established system of criminal justice."[317]

Law enforcement has relied on various forms of DNA testing since the 1980s.[318] Because so much of human DNA is identical, modern DNA testing focuses on key genetic sequences known as short tandem repeats (STRs) where human genetic patterns tend to vary widely.[319] Local, state, and federal law enforcement laboratories examine DNA gathered from convicted criminals, arrestees, and prior crime scenes and record the STRs appearing in twenty key loci in a profile. In addition to storing these profiles in their own databases, laboratories may upload them to the national DNA database authorized by Congress in 1994, known as the Combined DNA Index System (CODIS).[320] Laboratories can then compare the STRs contained in a DNA sample collected from an arrestee or a crime scene against the STRs appearing in the profiles stored in CODIS or a local or state database to determine the extent to which they match.[321]

DNA testing can yield three types of information. First, DNA can reveal medical information about an individual, such as genetic predispositions or medical risk factors, although CODIS's design reduces this concern in the context of law enforcement. Because the loci included in CODIS profiles do not have any known link to any genetic disease or predisposition, the data contained in CODIS cannot reveal medical information about any individual.[322]

---

315. *Id.* at 55; *accord King*, 569 U.S. at 460–61, 442 (noting that DNA testing allows "the police [to] ensure that they have the proper person under arrest" and "just as important, . . . [to] prevent suspicion against or prosecution of the innocent" and calling "the utility of DNA identification in the criminal justice system . . . undisputed").

316. *King*, 569 U.S. at 456.

317. *Osborne*, 557 U.S. at 62.

318. *Id.*; *King*, 569 U.S. at 442.

319. *King*, 569 U.S. at 443. From 1998 to the end of 2016, CODIS profiles included thirteen loci but expanded to twenty starting in 2017. *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Nov. 22, 2024).

320. *King*, 569 U.S. at 444–45; *see also* 34 U.S.C. § 12592.

321. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 297–98 (2010).

322. *King*, 569 U.S. at 445, 464.

Second, DNA can serve as a unique biological identifier, much like a fingerprint, only with greater accuracy.[323] As the Supreme Court has recognized, comparisons of DNA samples that yield exact matches can confirm the identity of a person better than any other current technology.[324]

Third, partial DNA matches can reveal kinship information. An individual shares more DNA in common with a blood relative than a random person, and the ability to identify the perpetrator's family members can provide law enforcement with leads that can help them solve crimes. Concerns about familial searches have led some states to ban them altogether.[325] Beginning in 2008, some states began authorizing the reporting of inadvertent or spontaneous partial matches identified when a CODIS search failed to yield an exact match so long as certain criteria are met.[326] Although the federal CODIS does not permit the submission of intentional or deliberate familial searches intended from the outset to yield partial matches identifying people related to the perpetrator,[327] some states have adopted policies permitting law enforcement to conduct familial searches on state DNA databases, usually subject to strict procedural requirements.[328]

---

323. *Id.* at 459.

324. Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 62 (2009) ("It is now often possible to determine whether a biological tissue matches a suspect with near certainty.").

325. MD. CODE ANN., PUB. SAFETY § 2-506(d) (2009); D.C. CODE § 22-4151 (2009).

326. For example, California began permitting reporting of inadvertent partial matches in 2008 so long as the crime scene DNA profile comes from a single source, the case is unsolved and all investigative leads have been exhausted, and the agency and prosecutor commit to investigate the case further if the search turns up positive. *See, e.g.*, Memorandum from Edmund G. Brown Jr., Cal. Att'y Gen., to All California Law Enforcement Agencies and District Attorneys Offices, DNA Partial Match (Crime Scene DNA Profile to Offender) Policy (2008) [hereinafter California Partial Match Policy], https://perma.cc/TED3-YYPK. For an early survey of other states, see Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 767–69, 807 (2011).

327. *Combined DNA Index System (CODIS)*, FBI, https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis-2 (last visited Nov. 22, 2024) [hereinafter *FBI CODIS Home Page*].

328. In 2008, California authorized intentional familial matching so long as criteria similar to those required for reporting of inadvertent partial matches are met. California Partial Match Policy, *supra* note 326. Colorado, New York, Virginia, and Texas adopted similar policies. Memorandum from Ronald C. Sloan, Dir., Colo. Bureau of Investigation, DNA Familial Search Policy: CBI Policy Statement (Oct. 22, 2009), https://perma.cc/VX3S-BWTD; N.Y. COMP. CODES R. & REGS. tit. 9, § 6192.3(h) (2017); VA. DEP'T OF FORENSIC SCI., DFS DOCUMENT NO. 107-D100, POLICY RELATING TO ACCEPTANCE OF CASES FOR

DNA testing also requires two distinct sources of DNA. First, it requires a sample of DNA to compare against the profiles contained in the database. These are typically collected directly from the suspect when processed or from tissue abandoned at the crime scene or left behind in some public place.[329]

Second, DNA testing also requires a database of profiles against which the sample can be compared. This can be a federal or state CODIS database built around information routinely and legitimately collected by law enforcement. Increasingly, law enforcement is comparing samples against third-party databases of genetic material maintained by private companies such as 23andMe, Ancestry.com, or GEDMatch that offer to digitize, analyze, and store information about individuals' DNA. Such platforms, however, may also turn over access to such genetic information to law enforcement.

1. The Law Enforcement Conduct Factor (Factor 1)

As noted above, the Law Enforcement Conduct factor requires both an assessment of the propriety of the conduct in obtaining the DNA used for testing and whether the practice enables indiscriminate, dragnet searches. Law enforcement typically collects data samples when processing arrestees or from crime scenes. It is now settled law that collecting DNA directly from a suspect on processing is not considered abusive. Indeed, the Court held in *Maryland v. King*[330] that "taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment" when they have probable cause to believe that the arrestee has committed a serious crime.[331]

Similarly, DNA abandoned at a crime scene does not implicate the type of abusive governmental conduct that the Fourth Amendment was designed to curb. Law enforcement officials working at crime scenes are clearly in locations where they are authorized to be. Nor does this type of case-specific investigation represent the type

---

PERFORMANCE OF FAMILIAL DNA SEARCHING (2011), https://perma.cc/B68U-PKTD; Gary Molina, CODIS Program Manager, Tex. Dep't of Pub. Safety, Presentation on Texas Familial Search Policy (July 7, 2011), https://perma.cc/3MGK-GPMR. For more general surveys, see EMILY NIEDZWIECKI ET AL., ICF INT'L, UNDERSTANDING FAMILIAL DNA SEARCHING: COMING TO A CONSENSUS ON TERMINOLOGY 5–6 (2016), https://perma.cc/UH62-2Q6L (reporting that Arkansas, Washington, and West Virginia also permit familial DNA searches); *FBI CODIS Home Page*, *supra* note 327 (adding Florida, Michigan, Utah, Wisconsin, and Wyoming).

329. *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 858 (2006).

330. 569 U.S. 435 (2013).

331. *Id.* at 465–66.

of "too permeating police surveillance" that would raise constitutional questions.[332]

The use of abandoned DNA collected from locations other than crime scenes can raise greater concerns about government overreaching. For example, law enforcement has sometimes gone to considerable effort to obtain DNA samples from discarded cigarette butts or coffee cups or saliva spat onto a street or deposited on an envelope when sealing it.[333] Concerns about these practices recently led Maryland to adopt a statute requiring investigators seeking to obtain a covert DNA sample to notify the authorizing court, provide an affidavit about the necessity of the covert collection, explain how they will conduct the collection in a manner that avoids unduly intrusive surveillance, file reports every thirty days, and complete the effort within six months.[334]

Regarding the DNA used to generate the profiles contained in CODIS, these profiles are generated exclusively from DNA collected from crime scenes and those accused or convicted of crimes.[335] Some jurists have warned that the lack of Fourth Amendment protection for abandoned DNA risks allowing its eventual inclusion in CODIS.[336] Other courts have held that although that broader collection of DNA "may empower the government to conduct wide-ranting 'DNA dragnets' that raise justifiable citations to George Orwell," such claims remain fanciful so long as current law limits CODIS to DNA collected from those involved in criminal activity.[337]

The permissibility under the Law Enforcement Conduct factor would also depend on the scope of the surveillance. Any law enforcement efforts to use DNA testing to track the movements of people in public without individualized suspicion would raise greater constitutional concern.

Law enforcement's use of DNA testing to reveal an individual's kinship also raises Fourth Amendment questions. If law enforcement is conducting a search to reveal kinship information, the risk of dragnet-style, suspicionless searches depends on how much of a perpetrator's family tree law enforcement is trying to find. A search about a suspect's nuclear family presents less of a risk for suspicionless surveillance than searching for information about one's entire extended family. Running a search on someone's full extended family could inadvertently run against thousands of individuals, all

---

332. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

333. Joh, *supra* note 329 at 860–61 (2006).

334. MD. CODE ANN., CRIM. PROC. § 17-102(g) (2021).

335. *See supra* note 320 and accompanying text.

336. United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004) (en banc) (Kozinski, J., dissenting).

337. Johnson v. Quander, 440 F.3d 489, 499 (D.C. Cir. 2006).

of whom are likely not relevant for investigating the defendant.[338] Consider the case of the Golden State Killer. When the CODIS search failed to yield an exact match, law enforcement used a partial match to build a family tree that extended to cousins, which can cover several thousand people.[339]

If taken to extremes, kinship information can have similar qualities to the CSLI analyzed in *Carpenter*. As an initial matter, genetic information gives law enforcement access to a wealth of information about the relations of a person,[340] so law enforcement is no longer hindered by "a dearth of records and the frailties of recollection."[341] Indeed, the decision by one relative of a suspect to share her genetic data reveals further information about the suspect's other relatives. The potential for abuse based on the shared genetic material now runs against all relatives regardless of when or why they chose to upload their own genetic material to the platform, if at all. In addition, DNA databases represent retrospective records containing information long preceding law enforcement interest in particular suspects.[342] Concerns about law enforcement's use of private DNA databases recently led Maryland and Montana to adopt legislation restricting law enforcement's use of intentional familial searches.[343]

Reliance on third-party databases raises additional concerns. Unlike CODIS, which is necessarily limited to information about individuals linked to proven or alleged crimes, third-party databases include a wide range of people with no connection to any wrongdoing. The potential for wide-ranging, retrospective surveillance of a broad swath of the population not involved in the breaking of any laws

338. Joseph Zabel, *The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics*, 24 BERKELEY J. CRIM. L. 47, 89–90 (2019).

339. *Id.* ("Detective Paul Holes, the lead investigator in the [Golden State Killer] case, explained how wide a net they cast saying 'we are talking third, fourth and fifth cousins and more distant than that.' The average person has around 4,700 fifth cousins." (quoting Richard Winton et al., *The First Step in Finding Golden State Killer Suspect: Finding His Great-Great-Great-Grandparents on Genealogy Site*, L.A. TIMES (Apr. 27, 2018), https://perma.cc/AZ7K-953B).

340. *See, e.g.*, Heather Murphy, *Genealogists Turn to Cousins' DNA and Family Trees to Crack Five More Cold Cases*, N.Y. TIMES (June 27, 2018), https://www.nytimes.com/2018/06/27/science/dna-family-trees-cold-cases.html.

341. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

342. *Id.*

343. MD. CODE ANN., CRIM. PROC. §§ 17-102(d), (f), 103(a)(4) (2021) (enacted in 2021 and permitting familial DNA searches only on direct-to-consumer genomics databases that provide explicit notice and consent that law enforcement may use the database to investigate crimes and requiring written approval from third-party non-suspects before their DNA can be used in familial DNA searches); MONT. CODE ANN. § 44-6-104(2) (2021) (enacted in 2021 and requiring search warrants before conducting familial DNA searches on consumer DNA databases).

raises concerns similar to the ones raised by *Carpenter* about surveillance that "runs against everyone."[344] The current state of warrantless law enforcement access to third-party genetic databases, however, is evolving; for example, GEDMatch reduced the profiles available to law enforcement by 95%.[345] Contractual obligations that prevent warrantless searches can mitigate the concerns of arbitrary surveillance.

2. The Defendant Conduct Factor (Factor 2)

This factor turns on the defendant's role in making the genetic material used in the DNA test available to law enforcement and what she could reasonably infer would be the implications of those actions. As was the case with the previous factor, we will consider the DNA in the sample that is the focus of the test and the DNA in the database against which that sample is checked.

a. Exposure by the Defendant (Factor 2A)

Regarding the sample used as the basis of the test, any DNA collected directly by law enforcement raises no notice requirements. As with images given directly to law enforcement in the case of IRT and FRT, defendants providing a cheek swab are well aware that law enforcement is in possession of the DNA.

Samples drawn from abandoned DNA raise more complex issues. On the one hand, the Supreme Court has held that the Fourth Amendment does not protect material that defendants have discarded. For example, *Abel v. United States*[346] held that the FBI's seizure of materials abandoned in the wastebasket of a vacated hotel room did not violate the Fourth Amendment by drawing an analogy to the open fields doctrine.[347] *California v. Greenwood* similarly held that the Fourth Amendment does not protect garbage left for collection outside the curtilage of a home in part because defendants left their "refuse at the curb for the express purpose of conveying it to a third party"[348] and in part because leaving trash outside was

344. *Carpenter*, 138 S. Ct. at 2218.

345. Terry Spencer, *Use of Online DNA Databases by Law Enforcement Leads to Backlash and Website Changes*, PBS NEWS (June 7, 2019), https://www.pbs.org/newshour/nation/use-of-online-dna-databases-by-law-enforcement-leads-to-backlash-and-website-changes.

346. 362 U.S. 217 (1960).

347. *Id.* at 241 (citing Hester v. United States, 256 U.S. 57, 58 (1924)).

348. California v. Greenwood, 486 U.S. 35, 40 (1988); *accord id.* at 41 (analogizing discarding trash to the voluntary conveyance of numbers to a telephone company found to be unprotected by the Fourth Amendment in Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

tantamount to leaving it in plain view.[349] Concerning the sample, the actions of the defendant thus militate against unconstitutionality, subject to one key additional consideration. *Abel* and *Greenwood* both involved refuse that defendants had voluntarily and intentionally discarded. In the case of abandoned DNA, defendants may not know that they abandoned it in the first place.[350] The Court's precedents on the third-party doctrine and plain view doctrine, on which its abandoned property decisions are based, turn on the fact that the defendants assumed the risk of exposing the searched data.[351] Because abandoning DNA is involuntary, it is harder to say that the defendant assumed the risk that that material might no longer be private.

Regarding genetic material used to construct the DNA database, to the extent that it was provided by the defendant when arrested for a prior crime, it cannot be said to give rise to concerns about fair notice. Moreover, exact matches to DNA that defendants voluntarily shared with third-party databases are also the direct result of voluntary actions on their part.

Familial searches pose bigger challenges. In those cases, the DNA leading to the partial match was provided by a relative, not the defendant. As a result, it is hard to regard the presence of that DNA in the database as the result of actions of which defendants had fair notice and over which they had control.[352]

b. The Reasonableness of Inferences Drawn from the Conduct of the Defendant (Factor 2B)

Even if the DNA in the sample or the database was the result of affirmative acts by the defendant, the second factor asks what the defendant could reasonably have expected those actions to reveal. Regarding the sample, any reasonable defendant should fully expect that any DNA sample provided directly to law enforcement could be

---

349. *Id.* at 39 (relying on Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), and California v. Ciraolo, 476 U.S. 207, 211 (1986), among others).

350. Joh, *supra* note 329, at 859 ("'Abandoned DNA' is any amount of human tissue capable of DNA analysis and separated from a targeted individual's person inadvertently or involuntarily, but not by police coercion.").

351. *Greenwood*, 486 U.S. at 41 ("Furthermore, as we have held, the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. . . . Again, we observed that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" (quoting *Smith*, 442 U.S. at 734–44)).

352. Murphy, *supra* note 321, at 337 ("After all, we cannot choose the persons with whom we share our genetic code. In some cases, the relative may have entirely disavowed the wayward convicted offender whose profile is in the database, or not even know of his or her identity. In light of the involuntariness and intractability of the genetic link, then, it seems indefensible to claim a voluntary relinquishment of privacy by the relative on account of mere biology.").

used for DNA testing. The inferences fairly drawn regarding abandoned genetic material are less clear. The fact that collecting abandoned DNA is not in "general public use" makes it harder to find that defendants could reasonably expect genetic traces left in public places could be used as the basis for a DNA test. The fact that this abandoned genetic material is plentiful leaves open the possibility that future advances in the ability to collect discarded DNA could lessen defendants' reasonable expectations of privacy if such searches become more common.

A similar analysis applies to third-party DNA databases. Defendants who submit their genetic material to private forensic genealogy services should be aware of the possibility that it may be used in a DNA test unless the database provides legal assurances against the practice in the absence of a court order.

Regarding familial searches of third-party databases, the proliferation of services like 23andMe and Ancestry.com makes it increasingly reasonable for defendants to expect that some third-party genetic database may contain DNA provided by a close enough relation to permit identifying them. Societal understanding of genetic privacy, the adoption of genealogy services, and new use cases for such familial DNA will undoubtedly influence this factor as DNA profiling technology advances in the years to come.

3. The Information Sensitivity Factor (Factor 3)

The sensitivity of information gathered from DNA profiling depends on the type of information that law enforcement gleans from the use of the technology. The information yielded by DNA testing is much like the identity information provided by fingerprinting, which the Supreme Court has noted does not involve "probing into an individual's private life and thoughts,"[353] with lower courts turning that dictum into holding.[354] The Supreme Court similarly relied on that language when holding that requiring defendants to provide voice exemplars did not implicate the kind of private information that implicated the Fourth Amendment.[355] In addition, *Maryland v. King* held that DNA testing purely for identification purposes without analyzing any genetic traits "did not intrude on [the defendant's] privacy in a way that would make his DNA identification unconstitutional."[356] These precedents establish that identification information provided by DNA testing is not sufficiently sensitive to affect the Fourth Amendment balance.

353. Davis v. Mississippi, 394 U.S. 721, 727 (1969).

354. *See, e.g.*, Rodgers v. Johnson, 174 F. App'x 3, 5 (3d Cir. 2006); United States v. Sechrist, 640 F.2d 81, 86 (7th Cir. 1981); United States v. Sanders, 477 F.2d 112, 113 (5th Cir. 1973).

355. United States v. Dionisio, 410 U.S. 1, 15 (1973).

356. Maryland v. King, 569 U.S. 435, 438 (2013).

Kinship information revealed by DNA testing is only slightly more sensitive than identity information. Contacting relatives of a suspected felon has long been an accepted law enforcement technique. Moreover, the increasing availability of information on the internet and the growth of services to help people mine it to construct family trees suggests that this information has become less sensitive over time. That said, genetic testing's ability to identify otherwise unidentifiable relatives may have the practical effect of reducing the practical obscurity that used to protect certain types of information from surveillance, the weakening of which may have Fourth Amendment implications.[357]

4. The Societal Impact Factor (Factor 4)

DNA profiling can be useful for identifying suspects or generating leads. The benefit to law enforcement, however, should be weighed against the adverse impacts of widespread DNA profiling in society.

a. The Social Benefits of More Effective Law Enforcement (Factor 4A)

The Supreme Court has recognized that DNA testing makes law enforcement more effective both in terms of more accurately identifying the guilty and in exonerating the innocent.[358] The mere fact that an investigative technique can help solve crimes is not by itself enough to make it constitutional. As noted above, however, such considerations appear to have greater purchase for crimes that conventional law enforcement techniques cannot solve.

Genetic material can be especially useful in solving cold cases or exonerating those who are wrongly convicted. Reports of how law enforcement has successfully used familial searches to solve cold cases are common. In addition to familial searches, abandoned DNA was crucial in finally arresting the Golden State Killer: Law enforcement used a DNA sample from the suspect's car door and another from a tissue in the trash that the suspect left for garbage collection.[359] The warrantless collection of abandoned DNA or data from a forensic genealogy service may help law enforcement more efficiently identify suspects in such hard-to-solve cases.

---

357. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)). For the seminal statement on practical obscurity, see *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 762 (1989).

358. *See supra* notes 315–17 and accompanying text.

359. Melody Gutierrez, *Golden State Killer Suspect's DNA Taken from Car as He Shopped at Hobby Lobby*, S.F. CHRON. (June 2, 2018), https://www.sfchronicle.com/crime/article/Golden-State-Killer-suspect-s-DNA-taken-from-12961700.php.

To weigh the benefits against potential distortions to society, the Department of Justice published DNA profiling guidelines in November of 2019 that permit law enforcement to query a genetic database for cases of unsolved violent crime or unsolved cases with human remains.[360] By specifying that DNA profiling should only be used for a certain class of crimes, this interim policy corroborates the notion that DNA profiling can be a powerful tool for solving crimes but must be used with caution. In addition, this policy demonstrates the result-oriented nature of the warrant requirement captured in this factor. We might consider certain crimes to be more serious than others, and we might prefer the use of certain technologies only in the case of more serious crimes.

b. The Social Costs of Avoidance Behavior (Factor 4B)

Each case of DNA profiling that we have considered has a different potential distortion on society when and if widely deployed. First, DNA profiling based on data collected directly from the defendant has limited distortions to our behavior in society because it is usually applied in controlled settings with the defendant.

Second, DNA profiling based on abandoned genetic material does not significantly affect our behavior in society at present because we do not believe this technique to be either effective or pervasive with the current generation of technology. If law enforcement could successfully collect our abandoned DNA to track our movements, however, this could create even more serious distortions to our behavior in society than facial recognition in public view. To avoid involuntarily leaving behind any trace of DNA, one would need to never leave her house or choose to wear protective gear in public, both of which are actions whose impact would outweigh the benefits of using forensic genealogy.

Third, DNA profiling based on third-party databases might less severely affect our behavior in society because individuals could selectively opt-in to databases that do not contractually prohibit warrantless access to data.

Lastly, DNA profiling based on familial searches may not create strong distortions to our behavior in society, primarily because a change in behavior on the part of the defendant would not necessarily make any difference in changing a relative's inclination to share their DNA.

5. Summation

The framework reveals that the reasonableness of a search with DNA profiling is categorically rooted in different Fourth Amendment concerns than a search that uses FRT or IRT, and different uses of

360. U.S. DEP'T OF JUST., INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING 4 (Nov. 1, 2019), https://perma.cc/H4DQ-K3R5.

DNA profiling, themselves, are each motivated by different factors as well. For DNA profiling from third-party databases or family members, the Information Sensitivity factor (Factor 3) dominates the analysis, especially in the cases of broad family tree constructions. For searches that use abandoned DNA, the non-routine use of this approach increases a reasonable expectation of privacy in involuntarily shed genetic material. If technology improves to make this approach more efficient, societal expectations about the reasonableness of an expectation of privacy in abandoned DNA (Factor 2B) might begin to erode as the technology becomes more generally used. The surveillance concerns around the indiscriminate use of this source of information (Factor 1) and the ensuing chilling effect on our movements and sense of liberty (Factor 4B), however, might counterbalance the trend.

III. SYNTHESIS OF FRAMEWORK

In applying the framework to each of the three case study technologies, we demonstrate how it can reveal our underlying motivations for why a search might violate the Fourth Amendment. We provide a summary table of this analysis, in which we consider six workflows based on the case study technologies. For FRT, we consider the use of FRT solely for identification and FRT for tracking the defendant's movements with location data. For IRT, we consider the use of IRT as it exists today, which performs best over short standoff distances and in controlled settings, and separately consider long-range iris recognition. For DNA, we consider DNA profiling from abandoned DNA separately from the other sources of DNA to highlight some unique perspectives that arise from abandoned DNA collection. Across each of these technologies, we see that the outcome from the framework varies in each factor. The variance in results indicates that our belief that law enforcement should get a warrant for the use of each of these technologies is rooted in different underlying concerns about the Fourth Amendment.

TABLE 1: HOW STRONGLY DOES EACH FACTOR MOTIVATE THE ULTIMATE DECISION THAT A SEARCH IS UNREASONABLE?

	1	**2A**	**2B**	**3**	**4A**	**4B**
FRT Identification	Low	Low	Low	Med	Med	Med
FRT Tracking	High	Low	Med	High	Med	High
IRT	Low	Low	Low	Low	Med	Low
Long Range IRT	High	Low	Med / High[361]	Med	High	Med
DNA	Low	Low[362]	Low	Med	Low	Low
Abandoned DNA	High	Low[363]	Med	Med	Low	High

First, this analysis shows that the conduct of law enforcement (Factor 1) drives the core of the Fourth Amendment's protection against police power. The more likely that law enforcement is conducting a search either in a place they have no right to be or in a manner that evokes the arbitrary, suspicionless searches under general warrants, the more likely this factor will push the ultimate decision about a search towards unreasonableness.

For the two FRT workflows considered, the conduct of law enforcement pushes searches toward unreasonableness when law enforcement has access to location data. FRT lets law enforcement aggregate such location data to analyze the defendant's pattern of life, and this cheap and effective approach to surveillance increases the potential for suspicionless, dragnet searches. A similar reasoning holds for IRT. Technological limitations in noncooperative IRT prevent law enforcement from using rich location metadata because IRT is only performant at low standoff distances. With long-range IRT, however, law enforcement will have access to more meaningful location data, which in turn elicits concerns about dragnet surveillance. For most workflows with DNA, such suspicionless

361. Medium for data from third-party databases due to the slow but increasing proliferation of private iris scan databases. High for data from public view due to a novel use of long-range iris recognition, in the face of which we might still afford the defendant a legitimate expectation of privacy in public.

362. This might be high in the case that law enforcement uses a family member's DNA—not that of the defendant—to create the family tree, and society accepts the defendant's claim to an expectation of privacy as legitimate.

363. *Id.*

surveillance concerns are usually limited. If DNA can be easily collected, as we outlined in the case of abandoned DNA collection, this might allow law enforcement to perform suspicionless surveillance more easily.

Second, the application of the framework to these technologies shows that actions of the defendant (Factor 2)—what was once the threshold question in an analysis of a Fourth Amendment search—fail to adequately capture the variation in why the Court finds searches unreasonable. Even though an analysis of the conduct of the defendant (Factor 2A) builds on notions of notice and fairness, in almost all of the case study technologies we considered, the defendant's actions alone decrease her expectation of privacy. Only in the case of familial DNA searches, where law enforcement uses a family member's DNA to build a family tree, could the defendant maintain a legitimate expectation of privacy undiminished by her own actions. The defendant's actions are not dispositive in understanding her expectations of privacy, nor are they enough alone to base our decision about whether a search is reasonable.

Analyzing the societal expectations about the defendant's conduct (Factor 2B) elucidates the impact of technological evolution on societal expectations of privacy: Specifically, under this factor, we see that the proliferation of a technology leads to nonprotection under the Fourth Amendment.[364] When law enforcement first uses a new technology to conduct a search, society might accept as reasonable a claim to an objective expectation of privacy from the use of that technology.[365] As the technology falls into more routine and public use, however, societal expectations of privacy from this technology decrease.[366]

For the two FRT identification and FRT tracking, we might have found the use of FRT to identify faces novel and uncommon, but today, the use of FRT is far more common. To go one step further and aggregate location metadata by the faces in these images, however, is not a common application of FRT in public use. This drives the distinction in the results for this factor between FRT with location

364. In fact, the Justices have often recognized this principle as well. In his dissent to *Kyllo*, Justice Stevens wrote that general public use standard "is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available." Kyllo v. United States, 533 U.S. 27, 47 (2001) (Stevens, J., dissenting). In his dissent to *Carpenter*, Justice Kennedy noted that many more people share their location data now than when *Knotts* was decided almost forty years ago, and so "expectations of privacy in one's location are, if anything, even less reasonable." Carpenter v. United States, 138 S. Ct. 2206, 2232 (2018) (Kennedy, J., dissenting).

365. *See, e.g.*, *Kyllo*, 533 U.S. at 33–36.

366. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 212–15 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 237–39 (1986).

data and without location data: Society would more likely accept as reasonable a claim to an expectation of privacy in location data aggregated by FRT than in just identification of a face in an image, if not also in aggerating images of faces. The reasoning for IRT is analogous. IRT with short standoff distances is in far more common use than long-range IRT. The most salient aspect of IRT as a case study technology is in revealing how the development of long-range IRT, as an example of any technological advance, impacts the reasonableness of a search under this factor. As long-range IRT improves and becomes more widely adopted, societal expectations around the conduct of the defendant will tend towards nonprotection because the defendant will have better notice of the technology's general public use.

In the case of DNA profiling, law enforcement has long used DNA as forensic evidence, and society would likely not accept as reasonable claims to expectations of privacy from the use of technology that can match DNA samples. In addition, with the proliferation of forensic genealogy services, our expectations of privacy in our kinship information may also begin to decrease. It appears as though this factor creates a one-way ratchet to nonprotection as technology gets more widely adopted. In his dissent to *Carpenter*, Justice Gorsuch arrives at the same conclusion about the applicability of the third-party doctrine to genetic databases.[367] The conduct of the defendant, coupled with the proliferation of genetic databases, does not afford the defendant a legitimate expectation of privacy based on her actions alone. It is only with the consideration of the other factors as well that we can counterbalance the nonprotection from the proliferation of technology and offer some legitimate expectation of privacy to the defendant in situations with widely deployed and potentially invasive technology.

In *Smith v. Maryland*, the Court recognized that an analysis predicated solely on the conduct of the defendant may be "inadequate."[368] The *Smith* Court foreshadowed that if the defendant's expectations of privacy had been "'conditioned' by influences alien to well-recognized Fourth Amendment freedoms,"

367. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting) ("Can [the government] secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*."). Justice Gorsuch, however, finds this outcome unexpected and continues, "[b]ut that result strikes most lawyers and judges today—me included—as pretty unlikely," criticizing the outcome of the third-party doctrine in this example. *Id.*

368. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) ("Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection.").

then "a normative inquiry would be proper."[369] Almost half a century after the *Smith* decision, we have become conditioned to new forms of technology that can easily be exploited for surveillance. In his dissent to *Smith*, Justice Marshall also remarked that this factor alone is not sufficient to analyze violations of privacy, writing that "to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections."[370] In *Carpenter*, the Court more fully articulates this failing of relying on conduct of the defendant (Factor 2) alone and includes a normative inquiry in its analysis.[371] It is this inquiry that we capture in our analysis of Information Sensitivity (Factor 3).

Third, the application of the framework shows that the considerations under the Information Sensitivity factor are also contextual: As certain types of information become more available or more sensitive in society, the results of this factor must accordingly evolve. For example, the use of telephones has significantly increased since the late 1970s when *Smith* was decided. Due to the proliferation of telephones, we are less likely to treat telephone numbers as a means of identification and do not place as much significance on our individual phone numbers as we might have in previous decades. This decreased social import in phone numbers would motivate a finding that a search is reasonable. For the data required for FRT, we consider the content of images with our faces. Such images reveal not only our likeness but also our friends, coworkers, and associations. For the data required for IRT, the data is usually a near-infrared image of one's iris, which is less revealing than the data for FRT. As such, under this factor, the sensitivity of the data for FRT more strongly contributes to a motivation that a search is unreasonable than it would for IRT. When location metadata is considered in addition to the data from these technologies, we must consider the comprehensiveness of the location data included. FRT is more

369. *Id.* ("In such circumstances, where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.").

370. *Id.* at 750 (Marshall, J., dissenting) ("More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications.").

371. *Carpenter*, 138 S. Ct. at 2219 ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

performant at long distances and in uncooperative settings than long-range IRT, so we likely can derive more meaningful and precise insights from aggregating location metadata in images with FRT. Thus, under this factor, we find that the use of location metadata increases the motivation to decide a search was unreasonable for both FRT and IRT. For DNA profiling, we might find the kinship information revealed by DNA more sensitive than any revealed identity information, but information about one's immediate family is not as personal today as it might have been in the past. If the digitization of public records and proliferation of genealogy platforms continues, the social import of this information may decrease, pushing this factor toward nonprotection as well.

Lastly, the greater emphasis on the impact on society when deciding whether a search is reasonable reflects an increasingly result oriented approach to the Fourth Amendment. Considering the first-order effects of deciding that a search is reasonable, that is, the creation of a per se rule that law enforcement can use such an approach in investigative procedures, we see that technological advancements that make law enforcement more accurate and efficient will motivate the decision about a search toward reasonableness. Moreover, the more likely the technology would be necessary and proportionate to solve the crime, the more likely we might permit its warrantless use. In our case study technologies, we see that DNA profiling has the lowest outcome under this factor. Identifying a suspect through a DNA sample can be an effective means of identification.[372] We are less likely to allow law enforcement to use FRT than IRT because FRT is known to have biases based on race, gender, and age. Such biases prevent law enforcement from achieving the intended "salutary effect"[373] of improving investigative practices to promote justice. FRT with location metadata and long-range IRT both further build on this reasoning. Both technologies may be disproportionate to the goal that law enforcement wants to achieve. For example, long-range IRT is not widely commercially deployed and has poor performance in noncooperative settings. Since there are likely other effective ways to identify a subject, we would likely not permit a search with long-range IRT to be conducted without a warrant that demonstrates its necessity. For this factor, we need to understand the context around the use of the technology in question to evaluate whether a warrant might be needed.

A social welfare-oriented analysis of societal impacts must also consider any second-order effects of deciding whether a search is reasonable. As law enforcement continues to perform searches in such a manner, an analysis of the societal impact of encouraging this law enforcement practice (Factor 4B) provides a lens into how such a

372. *See* Maryland v. King, 569 U.S. 435, 434 (2013).
373. *Id.* at 455.

practice affects societal behavior and norms. In evaluating this factor, we ask how willing we might be to accept the use of this technology and the impact it might have on society. The case study technologies highlight that we might be willing to tolerate improving law enforcement practices with technology to some degree, especially if it is easy to avoid the impacts of the technology. For example, we can easily frustrate the police use of short-range IRT when we seek to avoid those searches because IRT typically requires voluntary cooperation. The impact of FRT on our behaviors is harder to ignore using such tactics. Beyond just frustrating the collection of the primary data, if the technology captures our movements in public, only ceasing to move in public would fully reduce the impact of potential dragnet surveillance. Thus, the outcome for FRT with location data is the highest of the three case study technologies that we considered. For DNA profiling workflows, we can control voluntarily giving our DNA either directly to law enforcement or a third party. Only in the case of law enforcement use of abandoned DNA would we have no choice but to restrict our movements in public to prevent the involuntary shedding of genetic material.

This framework and its application demonstrate that across cases, the Court's rationale for why a search is reasonable is not monolithic. There is no one standard for reasonableness.[374] Through this value-based framework, each factor elucidates a core value that both underlies and motivates our answer to the question of reasonableness. A rich collection of privacy-protective values—individual autonomy and liberty, fairness and notice, deterrence against suspicionless surveillance—can uniquely motivate each determination of why a court may find a search reasonable. By analyzing each factor separately, we can better understand how values of privacy motivate each distinct thread of reasoning and ultimately yield a balanced judgment about reasonableness under the Fourth Amendment.

374. *See* Kerr, *supra* note 1, at 506 ("The Supreme Court has not and cannot adopt a single test for when an expectation is 'reasonable.'").