

THE ARCHITECTURE THE COURT CANNOT BUILD: CHATRIE V. UNITED STATES AND THE CASE FOR FIDUCIARY GOVERNANCE OF GOVERNMENT DATA

Michael G. Leahy, J.D.

AUTHOR'S NOTE

Michael G. Leahy, J.D., is a practicing attorney with experience in privacy law and legislative drafting. He formerly served as Maryland's Secretary of Information Technology and Chief Information Officer and as President of the National Association of State Chief Information Officers. The implementation analysis in Part V draws on that experience. He is the architect of the Fiduciary Commons Framework, a body of model legislation operationalizing fiduciary governance of government data, digital identity, and algorithmic decision-making.

ABSTRACT

In Chatrie v. United States (2026), the Supreme Court held that police acquisition of cell-phone location data constitutes a Fourth Amendment search, categorically rejecting durational thresholds and identifying the government's "virtual panopticon" as the constitutional concern. But the Court remanded on particularity and probable cause without addressing whether the surveillance infrastructure itself is constitutionally permissible. This Article argues that the Fiduciary Commons Framework provides what Chatrie needs and the existing doctrinal toolkit lacks: a structurally grounded account of government's data obligations that does not depend on case-by-case balancing, technology-specific holdings, or the fiction of meaningful consent.

The Article demonstrates that the four dominant approaches to the Fourth Amendment in the digital context, the property model, the consent model, the third-party doctrine, and the mosaic theory,

each fail for reasons Chatrue illustrates simultaneously. It presents a fiduciary alternative grounded in the proposition that the government-citizen information relationship generates categorical constitutional obligations derived from the Fourth Amendment's text and structural purposes. It engages Justice Gorsuch's property-based concurrence in detail, resolving the tension between property and privacy approaches through trust law principles of inalienability. It then translates the framework's constitutional analysis into architectural mandates, including mandatory data sequestration and query-without-collection protocols, enforceable through structural injunctions. Three model statutes operationalizing these mandates have been drafted, and elements of two have been enacted in Utah. The Court named the panopticon. The framework dismantles it.

PART I. INTRODUCTION

In *Chatrie v. United States*, the Supreme Court held that police officers conduct a Fourth Amendment search when they acquire an individual's cell-phone location data from Google, even for a limited period and even though a third-party technology company holds the data.¹ The holding extends *Carpenter v. United States* along lines that *Carpenter* itself anticipated.² But the decision's significance lies less in the holding than in what the majority said on the way to reaching it.

Writing for a six-Justice majority, Justice Kagan identified the constitutional concern animating the decision in terms that transcend the geofence warrant context: the government, she wrote, "possesses a virtual panopticon with which to scrutinize its citizens' activities."³ The constitutional wrong, in the majority's formulation, inheres not in any particular exercise of surveillance capability but in the capability itself. The "sweep of the official invasion is not made less because the government, with the benefit of hindsight, can pinpoint exactly which few hours of movements it wants to review."⁴ Two hours of Location History data constitutes a Fourth Amendment search not because two hours of movement data is especially revealing (though it can be), but because the government's access to Location History gives it standing, comprehensive, retrospective surveillance authority over any individual in any place at any time.

The majority named the panopticon. It did not dismantle it.

Chatrie holds that accessing Location History is a search. It remands to the Fourth Circuit to determine whether the geofence warrant satisfied the Fourth Amendment's requirements of particularity and probable cause "at each stage of the search process."⁵ It does not address whether the surveillance infrastructure itself, as distinct from any particular search conducted within it, is constitutionally permissible. It does not specify the technical architecture government information systems must satisfy to comply with the constitutional principles the decision articulates. And it does not provide the comprehensive remedial framework, covering not just criminal investigations but the full range of government information practices, that the constitutional principle the majority has identified requires.

These are not failures of judicial ambition. They are limitations of judicial competence. The Court can impose warrant requirements on new technologies. It can constrain individual warrants through probable cause and particularity analysis. What it cannot do, through case-by-case adjudication in criminal suppression proceedings, is mandate the architectural redesign of government information systems. That task belongs to legislatures, informed by constitutional principles that courts articulate and enforce.

This Article argues that the Fiduciary Commons Framework provides what *Chatrie* needs and the existing doctrinal toolkit lacks: a structurally grounded account of government's data obligations that does not depend on case-by-case balancing, technology-specific holdings, or the fiction of meaningful consent.⁶ The framework rests on a proposition the *Chatrie* majority approaches without reaching: the government-citizen information relationship is fiduciary in character, generating categorical constitutional obligations derived from the Fourth Amendment's text and structural purposes. Those obligations, loyalty, care, confidentiality, and transparency, translate into specific architectural mandates that legislatures can enact and courts can enforce. Three model statutes operationalizing these mandates have been drafted, and elements of two have been enacted in Utah.⁷

The argument proceeds in six Parts. Part II provides a close analysis of the full *Chatrie* decision: the majority's four doctrinal moves, Justice Jackson's concurrence on the particularity requirement, Justice Gorsuch's property-based concurrence, and the two dissents. The analysis demonstrates that the decision simultaneously extends Fourth Amendment protection and exposes the structural limits of the doctrinal framework within which it operates. Part III examines why the four dominant approaches to Fourth Amendment analysis of government data practices, the property model, the consent model, the third-party doctrine, and the mosaic theory, cannot produce stable doctrine, using *Chatrie*'s reasoning to illustrate each failure mode. Part IV presents the fiduciary alternative: the proposition that facts about individuals are unownable commons requiring stewardship, that the government-citizen information relationship generates fiduciary obligations derived from the Fourth Amendment, and that these obligations resolve the doctrinal

instabilities *Chatrie* exposes. Part IV also engages Justice Gorsuch's property-based concurrence in detail, demonstrating that the fiduciary framework accommodates and completes his analysis through trust law principles of inalienability. Part V translates the fiduciary framework's constitutional principles into architectural mandates, showing how mandatory data sequestration, query-without-collection architecture, and structural injunction remedies provide the operational infrastructure the Court's holding requires but cannot itself specify. Part VI identifies state legislative pathways through which the framework's model statutes can be enacted, drawing on existing legislative traction in Utah and the broader multistate engagement the framework has generated. Part VII concludes by situating the framework within the distinction between constitutional interpretation and political implementation: the fiduciary account of government's data obligations is constitutionally required, not merely a policy preference, but its architectural realization is a legislative project that courts can mandate and enforce without themselves designing government information systems.

The doctrinal instabilities *Chatrie* exposes are not merely theoretical. They have direct consequences for the state officials responsible for building and maintaining the government information systems that must comply with whatever constitutional requirements the Court's evolving doctrine imposes. A state chief information officer reading *Chatrie* knows that accessing cell-phone location data through a geofence warrant is now a Fourth Amendment search. She does not know whether her state's integrated human services database, which aggregates citizen records across dozens of programs and permits thousands of credentialed employees to query comprehensive personal information without individualized judicial authorization, presents the same constitutional problem. The fiduciary framework provides the answer: it does, because the database architecture exhibits the same structural characteristics, discretionary power, comprehensive scope, standing authorization, and accountability evasion, that the Fourth Amendment was ratified to prohibit.⁸ And the framework's model legislation provides the architectural standards her systems must satisfy.

The Court named the panopticon. The framework provides the blueprint for its constitutional replacement.

PART II. THE DECISION: WHAT *CHATRIE* RESOLVES AND WHAT IT CANNOT

Chatrie v. United States is a richer decision than its holding might suggest. The majority's conclusion that accessing Location History constitutes a Fourth Amendment search extends *Carpenter* along predictable doctrinal lines. But the reasoning the majority deploys, the concerns the concurrences raise, and the objections the dissents lodge collectively illuminate a deeper structural problem that the holding itself does not, and cannot, resolve. This Part examines the full decision: the majority's four doctrinal moves, Justice Jackson's concurrence on the particularity requirement, Justice Gorsuch's property-based concurrence, and the two dissents. The analysis proceeds in the order most useful for the argument that follows, which is roughly the order of the opinions' structural ambition: from the majority's extension of existing doctrine, through Jackson's effort to push beyond it, to Gorsuch's attempt to replace it, and finally to the dissents' defense of the doctrinal status quo.

A. The majority's four doctrinal moves

Justice Kagan's opinion for the Court proceeds through four analytically distinct steps, each resolving a question *Carpenter* had left open or addressed only partially. Taken together, they significantly extend Fourth Amendment protection for digital location data. They also reveal, with increasing clarity, the limits of the doctrinal framework within which the majority operates.

1. *Carpenter* extended: Location History as the successor technology

The majority's first move is its most straightforward. Location History, the Court holds, implicates the same privacy interests as the cell-site location information at issue in *Carpenter*, and does so with greater force along every dimension the *Carpenter* Court found relevant.⁹ The comparison is quantitative on three axes: precision (Location History pinpoints location within

approximately twenty meters, compared to CSLI's sector of one-eighth to four square miles); frequency (Location History records location every two minutes for a daily average of 720 chartings, compared to CSLI's average of 101); and dimensional richness (Location History can estimate elevation, revealing which floor of a building a phone occupies, a capability CSLI lacks).¹⁰

But the majority does not rest on the quantitative comparison. It makes a subtler move that carries significant doctrinal weight: Location History, unlike CSLI, is "more the individual's own."¹¹ Users treat Location History as a personal journal of their movements, consulting and editing it for their own purposes. In this respect, the majority observes, Location History "resembles other private materials, think of emails, documents, photographs, or calendars, that even if stored on Google's servers, a user reasonably views as his own."¹² This is not merely a factual observation about user behavior. It is a doctrinal move that strengthens the reasonable-expectation-of-privacy holding by grounding it in the user's subjective relationship to the data, a relationship that carries normative weight independent of the data's precision or comprehensiveness. The majority is saying, in effect, that the constitutional protection extends not only because the data is revealing but because the individual reasonably understands it as belonging to him.

This observation will prove significant when the analysis turns to Justice Gorsuch's property-based concurrence. The majority and the concurrence agree that the individual's relationship to his Location History data is constitutionally meaningful. They disagree about why.

2. The duration threshold rejected

The majority's second move is its most doctrinally significant. *Carpenter* had reserved whether there exists "a limited period for which the Government may obtain" cell-phone location data "free from Fourth Amendment scrutiny."¹³ The Government argued that two hours of Location History falls within that constitutional gap, because short-term movements "reveal little about the details of [a person's] personal life."¹⁴ The majority rejects this argument categorically.

The reasoning proceeds on two levels. At the narrower level, the majority contests the Government's factual premise. Drawing on Justice Sotomayor's concurrence in *Jones*, the Court observes that "even short-term monitoring" can reveal "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations."¹⁵ The Court's catalogue of "indisputably private" destinations, from the psychiatrist's office to the criminal defense attorney, demonstrates that a single trip can be as revealing as a month of movements.¹⁶ And unlike a GPS device, Location History enables officers to focus on precisely those sites, to see, in a given time block, who appears.

At the broader level, the majority articulates a categorical principle: "Where the Fourth Amendment applies, it applies, regardless of 'the quality or quantity of information' the government obtains."¹⁷ The Court invokes *Kyllo's* analogy of the officer who "barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor": the Amendment "makes no exception" for minimal intrusions.¹⁸ It observes that the seminal wiretap case, *Katz* itself, involved only eighteen minutes of recordings.¹⁹ And it notes that the Government's durational approach would generate intractable line-drawing problems: "At what point, exactly, would a non-search become a search? In two hours, or six hours, or one day, or six days?"²⁰

But the passage that matters most for the argument this Article develops is the majority's identification of the structural wrong:

What creates that concern is that the government can access all of a cell-phone user's movements, in both public and private places; that it possesses a virtual panopticon with which to scrutinize its citizens' activities. The sweep of the official invasion is not made less because the government, with the benefit of hindsight, can pinpoint exactly which few hours of movements it wants to review.²¹

The constitutional wrong, in the majority's formulation, inheres in the surveillance capability, not in any particular exercise of it. The government "possesses" the panopticon regardless of how much data it demands in a given case. The durational bounds on the data actually

acquired are "more a practical benefit to the government than a limit on its intrusive powers."²² This passage represents the Court's closest approach to the proposition that the constitutional violation is architectural rather than transactional: that it is the existence of the surveillance infrastructure, not any particular search conducted within it, that offends the Fourth Amendment.

The majority does not follow this insight to its structural conclusion. It does not ask whether the existence of Google's centralized Location History database was itself a constitutional problem, or whether government's capacity to compel production from such a database constitutes the kind of standing, comprehensive, discretionary surveillance authority the Fourth Amendment was ratified to prohibit. Those questions lie beyond the doctrinal framework within which the majority operates. But the passage quoted above, and the categorical principle it embodies, point unmistakably toward the structural analysis this Article provides.

3. The third-party doctrine further eroded

The majority's third move addresses the Government's secondary argument: that the third-party doctrine, under which individuals lose Fourth Amendment protection in information they voluntarily share with others, precludes Chatrue's claim. *Carpenter* had refused to apply the doctrine to CSLI, reasoning that cell-phone location data is "qualitatively different" from the telephone numbers and bank records at issue in *Smith v. Maryland* and *United States v. Miller*, and that such data is "not truly 'shared' as one normally understands the term" given that cell phones are "indispensable to participation in modern society."²³

The Government attempted to distinguish Location History from CSLI on voluntariness grounds. CSLI is generated passively by the mere act of carrying a turned-on phone. Location History, by contrast, requires an "affirmative act" beyond powering up: the user must enable the service. Only about one-third of Google accountholders have done so, the Government argued, demonstrating that people can "live without" it.²⁴

The majority rejects this argument on three grounds, each more structurally ambitious than the last. First, at the factual level, the Court observes that Google "prompts a user, and repeatedly,

to turn on the service," often warning that the device "will not work correctly" without it, while failing to disclose how frequently location would be recorded, how precise the data would be, or how it might be provided to the government.²⁵ In these circumstances, the Court concludes, "it is hard to see how any user is, in the normal sense, 'sharing' with third parties a comprehensive catalog of his physical movements."²⁶

Second, at the doctrinal level, the majority identifies a parade of workability problems with the Government's approach. What percentage of users must sign up for a service before using it becomes "non-voluntary"? Would Fourth Amendment protection fluctuate as a service's popularity rises and falls? What if a feature is ubiquitous among one demographic cohort but not others? The Court's conclusion: "To ask all these questions about the Government's approach is to know that it is on the wrong track."²⁷

Third, and most consequentially, the majority identifies a structural flaw in the Government's entire analytic framework. The "app-by-app, feature-by-feature method of granting Fourth Amendment protection misapprehends the very nature of modern cell-phone use."²⁸ Virtually everything a person does on a smartphone requires an affirmative opt-in: sending an email on Gmail, uploading a photo to Google Photos, adding a calendar entry. Each of these activities results in sharing information with a third-party technology company. The Government's approach would strip Fourth Amendment protection from all of them, confining constitutional coverage to the bare act of carrying a turned-on phone. "But that," the majority observes, "is to imagine that all of us are living in dumb flip-phone days."²⁹

This passage carries implications far beyond the geofence warrant context. The majority is saying that the third-party doctrine cannot survive contact with the architecture of modern digital life, where virtually every meaningful interaction with a smartphone generates data held by third parties. The Court does not formally overrule *Smith* or *Miller*. But its reasoning confines those holdings to their original contexts and effectively precludes their extension to any data generated through ordinary smartphone usage.

4. The remand: the questions the Court cannot answer

The majority's fourth move is its most revealing, precisely because it is a refusal to move. Having held that accessing Location History constitutes a Fourth Amendment search, the majority declines to reach whether the geofence warrant satisfied the Amendment's requirements of particularity and probable cause "at each stage of the search process."³⁰ The Court notes that the warrant was "uncommon" and "multi-step," that the parties contest the legality of each stage, and that the Fourth Circuit never addressed these questions because it concluded no search had occurred.³¹ It remands for the Court of Appeals to decide "in the first instance."³²

This remand defines the structural gap the fiduciary framework fills. The Court can say that a search occurred. It can impose a warrant requirement. But it cannot mandate the database architecture that would prevent the surveillance capability from arising in the first instance. It cannot specify the technical standards that government information systems must satisfy to comply with the constitutional principles the decision articulates. And it cannot provide the comprehensive remedial framework, covering not just criminal investigations but the full range of government information practices, that the constitutional principle requires. Those tasks lie beyond the institutional competence of case-by-case adjudication.

B. Jackson on particularity: the general warrant rediscovered

Justice Jackson's concurrence, joined by Justice Sotomayor, goes where the majority would not: she would have held that the geofence warrant failed the Fourth Amendment's particularity requirement at steps two and three.³³ The concurrence is brief, but its doctrinal implications are substantial.

Jackson identifies two structural defects in the warrant. First, at both steps two and three, the warrant stated only that officers would "*attempt* to narrow down the list" of devices, without setting forth any criteria for doing so and without requiring that they actually narrow it.³⁴ Second, and consequently, "officers could obtain additional, sensitive information at steps two and three without having to convince a magistrate that there was probable cause to believe this particular

information would uncover evidence related to the crime."³⁵ The warrant left "too much to the discretion of the officer[s] executing the order," giving them what Jackson, invoking *Berger v. New York*, calls "a 'roving commission' to collect more data absent any justification to a magistrate."³⁶

The factual record vindicates Jackson's structural concern. When executing the warrant, officers initially sought unbounded data and identifying information from all nineteen devices identified at step one. "Nothing in the warrant prevented officers from obtaining this broad set of data; they narrowed the list only because Google insisted on it."³⁷ A private corporation, not the warrant, performed the constitutional function that the particularity requirement is designed to serve. Even the narrowed list proved overbroad: for three of the nine devices retained at step two, the location data revealed movements to and from residences, a school, and a hospital.³⁸ The warrant, Jackson concludes, "provided no 'judicial check' on law enforcement's determination that probable cause justified this intrusion."³⁹

Jackson's analysis illuminates three points that bear directly on the argument this Article develops. First, the "roving commission" language is the general warrant objection in modern dress. A warrant that authorizes officers to expand a search at their discretion, without returning to the magistrate for independent authorization of each expansion, is the digital analogue of the general warrants that James Otis denounced and the Fourth Amendment was ratified to prohibit.

Second, the fact that Google, not the warrant, constrained the officers' discretion demonstrates why architectural constraints cannot be left to voluntary corporate practice. Google chose to insist on narrowing. It was not constitutionally required to do so. A different company, or Google under different corporate leadership, might have complied with the officers' initial request for all nineteen devices without objection. Constitutional protections that depend on the business judgment of private technology companies are not constitutional protections at all.

Third, Jackson's emphasis on the particularity requirement provides a Fourth Amendment anchor for algorithmic accountability. If the warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized," then algorithmic processes that select targets for

heightened scrutiny, such as the narrowing decisions at steps two and three of the geofence protocol, require their own constitutional justification. The warrant cannot delegate that justification to the officers' unguided discretion, and it cannot delegate it to an algorithm's unexamined criteria. This principle, which Jackson identifies at the level of warrant procedure, has implications that extend to every algorithmic system through which government processes citizen data.

C. Gorsuch on property: the productive tension

Justice Gorsuch concurs in the judgment but would reach it by "a different route."⁴⁰ His concurrence is the decision's most analytically ambitious opinion, and the one that creates the most productive engagement with the fiduciary framework this Article proposes.

1. The argument

Gorsuch renews his critique of the *Katz* reasonable-expectation-of-privacy test, first articulated in his *Carpenter* dissent. The test, he argues, has "no basis in the Constitution's text or history," is empirically unknowable and normatively arbitrary, and has produced an "equally indefensible qualification called the third party doctrine" under which "the government may freely search a person's papers and effects without triggering any Fourth Amendment scrutiny so long as they are entrusted to the care of someone else."⁴¹ The majority's approach, Gorsuch charges, amounts to "I know it when I see it" jurisprudence.⁴²

In place of *Katz*, Gorsuch would consult the Fourth Amendment's text. Location History, he argues, qualifies as one of Chatrle's "effects," meaning his personal property. Chatrle held the rights to enjoy, manage, alter, dispose of, and exclude others from his location data. Google's terms of service referred to Location History as "your information." Chatrle could review, edit, export, and delete the data at will, and Google promised to protect it against unauthorized access.⁴³ These are the "sticks in the bundle of rights . . . commonly characterized as property," including what *Cedar Point Nursery v. Hassid* called the "most treasured" right to exclude.⁴⁴

Gorsuch reinforces this analysis with statutory and case law. Virginia's Computer Crimes Act classifies "computer data" as property. Texas, Georgia, and numerous other states have comparable provisions.⁴⁵ Colorado's *People v. Seymour* held that law enforcement's copying of a defendant's search history "meaningfully interfered with his possessory interest in that data."⁴⁶ The Cato Institute brief reported that more than half of states now treat digital records and data as personal property.⁴⁷

Critically, Gorsuch argues that entrusting property to a third party does not extinguish the owner's Fourth Amendment interest. The valet analogy: "[T]oss your keys to a valet at a restaurant" or "[a]sk your neighbor to look after your dog while you travel," and your property remains yours even though another person holds and uses it for agreed purposes.⁴⁸ Similarly, the fact that Google stored Chatrle's Location History on its servers and was free to use it for certain purposes does not convert his property into Google's, any more than a tenant's lack of fee simple title extinguishes his Fourth Amendment interest in his residence.⁴⁹

Gorsuch's closing paragraph is perhaps his most revealing. The majority, he observes, protects Location History, emails, and other cloud-stored data because "a user reasonably understands" those things "as his own." "Put another way," Gorsuch writes, "they are his effects." And the majority holds those effects protected "even though stored on Google's servers." "Put another way, entrusting your effects to a third party for certain agreed purposes doesn't mean they are no longer yours."⁵⁰ Gorsuch is reading the majority's privacy analysis as a property analysis in disguise, groping toward the more "coheren[t]" framework he advocates.⁵¹

2. What the property analysis reaches and what it does not

Gorsuch's analysis is compelling on its own terms. It reaches the correct result for the individual's relationship to his data records, and it does so through textual and historical reasoning that avoids *Katz*'s normative indeterminacy. But the property model cannot reach three structural problems that any adequate Fourth Amendment account of government data practices must address.

First, facts are discovered, not created. The underlying facts that Location History records, the places Chatrue went and the times he was there, exist independent of any recording. What Chatrue holds is the record, not the fact. This distinction matters because government generates its own records of citizen facts through administrative processes: tax filings, license applications, benefits enrollment, law enforcement databases. A property-based account of Location History cannot explain why the government's own databases, populated through mandatory processes rather than custodial entrustment, are constitutionally problematic. The fiduciary framework can, because it locates the constitutional obligation in the governmental relationship rather than the custodial chain.

Second, property can be alienated. If location data is property, it can be transferred through contract. Users routinely "consent" to data collection through terms of service. Gorsuch acknowledges that Google was "free to use [Chatrue's data] for certain purposes" pursuant to their agreement.⁵² But a property model, taken to its logical conclusion, would permit citizens to alienate their Fourth Amendment interests through clickwrap agreements, a result that is constitutionally untenable when the "consent" occurs under conditions of informational asymmetry and practical compulsion. This is the inalienability problem, and it requires a structural solution. Trust law provides one. The Restatement (Third) of Trusts recognizes that certain interests are held in trust precisely because they cannot be safely alienated: spendthrift provisions exist to protect beneficiaries from their own improvident dispositions.⁵³ *Illinois Central Railroad Co. v. Illinois* established that the state cannot alienate public trust resources because they are "held in trust for the people."⁵⁴ Frankel's categorical fiduciary duty theory holds that fiduciary obligations arise from the structure of the relationship, not from contractual specification, and cannot be waived when the structural conditions generating them persist.⁵⁵ Sitkoff's agency-costs framework reaches the same conclusion through efficiency analysis: mandatory fiduciary duties minimize the losses that arise when discretionary authority is delegated under conditions of power asymmetry.⁵⁶ These authorities establish that the individual's relationship to his personal data is custodial rather than proprietary: he holds it in a capacity that generates obligations he cannot unilaterally extinguish.

Third, and most fundamentally, Gorsuch's analysis protects Chatrle's data against government access through a third party. It does not reach the government's own integrated databases. When government collects data through mandatory administrative processes, no third-party custodian mediates the relationship. The property model's explanatory power depends on the custodial chain: Chatrle entrusted his data to Google; the government searched Google's servers; Chatrle's property interest makes that search constitutionally cognizable. But when the data originates in government processes, no entrustment occurs, no custodial chain exists, and the property analysis has no purchase. The fiduciary framework reaches both contexts because it derives the constitutional obligation from the government-citizen relationship itself, not from the architecture of data custody.

3. The convergence

The productive tension between Gorsuch's property analysis and the majority's privacy analysis is not, at bottom, a disagreement about outcomes. Both reach the same result: Chatrle's Location History is constitutionally protected against warrantless government access. The disagreement concerns the doctrinal path, and the fiduciary framework resolves the tension by showing that both paths point toward the same structural reality.

Gorsuch reads the majority's privacy analysis as crypto-property: the Court protects Location History because the user "reasonably understands" it "as his own." The majority reads its own analysis as irreducibly about privacy: constitutional protection extends because the surveillance capability threatens the "privacies of life" the Fourth Amendment was designed to safeguard.⁵⁷ Both readings are partially correct. The individual does have a custodial interest in his data records (Gorsuch's insight). And the surveillance capability does threaten the constitutional relationship between government and citizen regardless of who holds the data (the majority's insight). The fiduciary framework accommodates both because it recognizes the individual as the primary trustee of facts about himself, a relationship that generates both the custodial interest Gorsuch identifies and the structural obligation the majority intuits.

Gorsuch's valet analogy, intended to support the property analysis, illustrates the point. Tossing your keys to a valet creates a bailment, a custodial relationship that generates fiduciary obligations. The valet must return the car, must not use it for unauthorized purposes, and must exercise reasonable care in its custody. These are not property obligations; they are relational obligations arising from the structure of the entrustment. The fiduciary framework extends this relational logic to the government-citizen information relationship, with the additional structural feature that the citizen cannot exit the relationship or bargain over its terms.

D. The dissents: what they concede

Justice Alito's dissent, joined by Justice Thomas as to Part I and by Justice Barrett as to the substantive Fourth Amendment analysis, mounts three distinct challenges. Each, on examination, concedes a premise the fiduciary framework requires.

First, Alito charges that the majority has issued an "advisory opinion" because the good-faith exception to the exclusionary rule will almost certainly save the conviction on remand.⁵⁸ The objection may be procedurally sound: the majority effectively concedes that the case's outcome is unlikely to change.⁵⁹ But the charge highlights a structural problem that the dissent does not acknowledge. If the Court can reach surveillance architecture only through exclusionary rule litigation, judicial enforcement of the Fourth Amendment will always be sporadic, retrospective, and dependent on the fortuity that a criminal defendant raises a suppression motion, that the motion survives the good-faith exception, and that the resulting holding extends beyond the specific technology at issue. Alito's objection is thus an inadvertent argument for the framework's legislative approach: proactive architectural mandates enacted through model legislation, enforceable through private rights of action and structural injunctions, rather than case-by-case criminal procedure adjudication.

Second, Alito observes that the geofence procedure at issue is "now-obsolete" because Google moved Location History to device-level storage in July 2025.⁶⁰ The majority acknowledges this change in footnote 3.⁶¹ Alito intends this as a criticism: the Court is deciding a question about a

technology that no longer exists. But the observation inadvertently concedes the fiduciary framework's central architectural premise. Google's shift to device-level storage demonstrates that query-without-collection, the principle that verification does not require centralized data retention, is operationally viable at scale. The world's largest data company voluntarily adopted the architecture the PDTA would constitutionally mandate. If the technological capability exists to prevent the constitutional violation, the constitutional argument for mandating that capability strengthens.

Third, Alito charges that the majority's decision "sheds *Carpenter*'s self-imposed boundaries and further destabilizes longstanding Fourth Amendment jurisprudence."⁶² This charge has force. *Carpenter* reserved the short-duration question, and the majority has now resolved it in a way that extends Fourth Amendment protection significantly. But Alito's proposed alternative, deference to the third-party doctrine and *Carpenter*'s self-imposed limitations, cannot produce the doctrinal stability he seeks. The instability arises not from the majority's willingness to extend *Carpenter* but from the transactional premises that all existing doctrinal approaches share: the assumption that the Fourth Amendment addresses discrete search events rather than surveillance architecture, and the resulting inability to provide structural remedies for structural constitutional violations. The fiduciary framework provides the stable doctrinal foundation that neither *Carpenter*'s case-by-case approach nor Alito's doctrinal conservatism can deliver, because it locates the constitutional wrong at the level of the governmental relationship rather than the individual search event.

Justice Barrett writes separately to emphasize that even under *Carpenter*'s framework, the limited duration and the geofence warrant's built-in narrowing process distinguish this case from *Carpenter*'s seven-day comprehensive surveillance.⁶³ Her dissent largely tracks the substantive analysis in Alito's Part II. The separate filing principally signals that the doctrinal disagreement over *Chatree*'s extension of *Carpenter* may prove narrower than Alito's rhetoric suggests: Barrett joins the substantive Fourth Amendment analysis but does not join Alito's jurisdictional challenge or his broader critique of the Court's institutional role.

PART III. WHY EXISTING FRAMEWORKS REMAIN INADEQUATE

Part II demonstrated what *Chatrie* resolves and what it leaves open. This Part examines a prior question: why the doctrinal toolkit the Court employed, and the alternative frameworks the concurrences and dissents proposed, cannot produce stable answers to the problems the decision identifies. The inadequacy is not a matter of judicial error or insufficient ambition. It is structural. Each of the four dominant approaches to Fourth Amendment analysis of government data practices rests on transactional premises that digital surveillance architecture has rendered obsolete. *Chatrie* illustrates all four failure modes simultaneously, demonstrating that the instability the decision both addresses and perpetuates arises from the premises the approaches share rather than from any deficiency specific to one of them.⁶⁴

A. The property model's category error

The property-based approach to personal data, most fully developed in Justice Gorsuch's *Chatrie* concurrence and in the emerging state statutory framework he catalogues, treats digital data as personal property subject to the Fourth Amendment's protection of "effects."⁶⁵ As Part II demonstrated, this analysis reaches the correct result for the individual's custodial relationship to data records held by third parties. It cannot, however, provide a general account of the constitutional relationship between government and citizen data.

The difficulty is foundational. Facts about individuals, where a person went, what services she received, what taxes she paid, are discovered, not created. They exist independent of any recording. The Supreme Court recognized this principle in *Feist Publications, Inc. v. Rural Telephone Service Co.*, holding that facts cannot be copyrighted because they are not the product of original authorship.⁶⁶ *Feist* is a copyright decision, and extending its holding to Fourth Amendment property analysis requires care. But the underlying insight, that facts belong to no one because they are features of the world rather than products of human effort, has structural implications that reach beyond copyright doctrine. If the facts Location History records are not *Chatrie*'s property (they are

features of the physical world: he was at a particular place at a particular time), then what *Chatrie* holds is the record, not the fact. The record may be his effect. The fact is not.

This distinction matters because government generates its own records of citizen facts through mandatory administrative processes. The Department of Motor Vehicles records the fact that a citizen resides at a particular address. The Internal Revenue Service records the fact that she earned a particular income. The benefits agency records the fact that she received a particular service. These records are not entrusted to government by the citizen in any custodial sense; they are generated by government through the exercise of sovereign authority. A property model that protects *Chatrie's* Location History because he entrusted it to Google cannot explain why the government's own integrated databases, populated through compulsory processes, are constitutionally problematic. Yet the constitutional concern is the same: comprehensive, standing, discretionary access to the intimate details of citizens' lives.⁶⁷

The property model's further vulnerability, identified in Part II's inalienability analysis, compounds the category error. If data is property, property law's default rules permit alienation. The consent-through-terms-of-service problem, to which this Part now turns, is a direct consequence of treating data as a commodity rather than recognizing the relational obligations its custody generates.

B. The consent model's constitutional failure

The consent-based approach holds that individuals who voluntarily disclose information to third parties assume the risk that the information will be conveyed to the government, and thereby forfeit Fourth Amendment protection. The *Chatrie* majority's rejection of the Government's "optional add-on" argument is the decision's most thorough engagement with the consent model's failures.⁶⁸

The majority identifies three levels of failure. At the most granular level, consent to Location History is not meaningfully informed: Google prompts users repeatedly, warns that devices will not "work correctly" without the service, and fails to disclose the frequency, precision,

and potential governmental use of the data collected.⁶⁹ At the doctrinal level, the consent model generates unworkable line-drawing questions: what adoption percentage makes a service "non-voluntary," and does Fourth Amendment protection fluctuate with market trends?⁷⁰ At the structural level, the app-by-app, feature-by-feature approach to constitutional protection "misapprehends the very nature of modern cell-phone use," where virtually every interaction requires some form of opt-in and generates data held by third parties.⁷¹

These failures are real, and the majority's analysis of them is incisive. But the majority's critique does not reach the consent model's deepest deficiency, which becomes visible only when the analysis moves from the commercial context (citizen-to-Google) to the governmental context (citizen-to-state). Citizens cannot exit government jurisdiction. They cannot decline to file tax returns, refuse to obtain driver's licenses, or opt out of regulatory compliance. The information they provide to government is furnished under legal compulsion as a condition of receiving services, obtaining licenses, and complying with requirements that carry penalties for noncompliance. In this context, consent is not merely uninformed or procedurally deficient. It is structurally impossible. The concept of voluntary disclosure presupposes the possibility of withholding, and the government-citizen relationship forecloses that possibility by design.⁷²

The *Chatrre* majority approaches this insight without reaching it. The Court's observation that the "point of carrying smartphones is to use what is on them" gestures toward the structural impossibility of meaningful consent in a technologically mediated society.⁷³ But the majority frames the problem as one of practical compulsion (people cannot realistically avoid smartphone features) rather than constitutional structure (citizens cannot constitutionally be required to forfeit Fourth Amendment protection as a condition of participation in civic life). The distinction matters. Practical compulsion can be ameliorated by better disclosure, more granular consent mechanisms, or technological alternatives. Constitutional structure cannot. The fiduciary framework locates the consent model's failure at the structural level, where it belongs.

C. The third-party doctrine's incoherence in the digital age

The third-party doctrine, first articulated in *United States v. Miller* and *Smith v. Maryland*, holds that information voluntarily conveyed to a third party loses Fourth Amendment protection because the conveying party has "assumed the risk" that the third party will disclose it to the government.⁷⁴ *Carpenter* declined to extend the doctrine to CSLI. *Chatrue* declines to extend it to Location History. Neither decision overrules *Miller* or *Smith*.

The result is a doctrine that no longer has a coherent domain of application. As the *Chatrue* majority demonstrates, virtually every interaction with a modern smartphone generates data held by third parties. Emails are stored on Google's servers. Photographs live in Apple's cloud. Calendar entries, document drafts, search histories, and messaging logs all reside with technology companies rather than on the user's device. If the third-party doctrine applied to these materials, the Fourth Amendment would protect almost nothing in the digital lives of the ninety-one percent of Americans who carry smartphones.⁷⁵ If it does not apply to them, as the majority's reasoning strongly implies, then the doctrine survives only for the narrow categories of information at issue in the 1970s cases that created it: bank records and pen register data.

Justice Gorsuch identifies this incoherence from the opposite direction. The third-party doctrine, he argues, "amounts to little more than a doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."⁷⁶ His proposed solution is to abandon *Katz* entirely in favor of a textual, property-based approach. But as Part II demonstrated, the property approach creates its own set of problems. Neither *Katz* nor its property-based alternative can produce stable doctrine when the underlying premise, that the Fourth Amendment addresses discrete transactions between identifiable parties, no longer describes the architecture of government surveillance.

The third-party doctrine's incoherence is a symptom rather than a cause. The cause is the transactional framework within which the doctrine operates. The doctrine asks whether a particular individual voluntarily disclosed particular information to a particular third party. When surveillance occurs through integrated databases that aggregate information from thousands of sources, many of them compulsory and most of them opaque to the individual, the transactional

question has no coherent answer. The fiduciary framework dissolves the question by replacing it with a structural one: does the government-citizen information relationship generate fiduciary obligations, and if so, does the government's information architecture satisfy them?

D. Mosaic theory and the line-drawing problem

The mosaic theory of the Fourth Amendment, developed in Justice Alito's concurrence in *Jones* and elaborated by Professors Gray and Citron, holds that sustained surveillance aggregates individually innocuous data points into a constitutionally significant composite.⁷⁷ The theory captures a genuine insight: the constitutional problem with modern surveillance is not any single data acquisition but the comprehensive picture that emerges from aggregation over time.

Chatrie's rejection of durational thresholds simultaneously validates and undermines the mosaic theory. The majority validates the theory's core insight when it observes that "even short-term monitoring" can reveal intimate details of a person's life.⁷⁸ But it undermines the theory's operational premise when it refuses to identify a durational threshold below which aggregation is constitutionally insignificant. If the Fourth Amendment applies regardless of "the quality or quantity of information" obtained, then the mosaic theory's central question, how much aggregation is too much, has no answer.⁷⁹

The mosaic theory's line-drawing problem is well documented in the post-*Carpenter* case law. Lower courts have reached inconsistent results in applying *Carpenter*'s principles to different surveillance technologies and different time periods, precisely because the aggregation threshold is indeterminate.⁸⁰ *Chatrie* resolves the duration problem by eliminating the threshold entirely for cell-phone location data. But elimination is not the same as principled resolution. The majority's categorical approach works for Location History because the technology's comprehensiveness makes any temporal line arbitrary. It does not provide a framework for evaluating less comprehensive surveillance technologies, surveillance conducted through government's own databases rather than third-party compulsion, or the cumulative effect of multiple surveillance programs that individually fall below whatever threshold the Court might eventually recognize.

The fiduciary framework asks a different question. Rather than asking how much aggregation is too much, it asks whether the government's information architecture exhibits the structural characteristics of the general warrants the Fourth Amendment was ratified to prohibit: discretionary power, comprehensive scope, standing authorization, and accountability evasion.⁸¹ This four-factor test, derived from James Otis's denunciation of the writs of assistance, asks a structural question about the governmental relationship rather than a quantitative question about the volume of data. The test produces determinate answers because it evaluates the architecture of surveillance authority rather than the output of particular surveillance events.

E. The common failure

Chatrie does not merely illustrate these four failure modes sequentially. It illustrates them simultaneously, demonstrating that the instability is structural rather than doctrinal.

The majority extends *Carpenter's* privacy analysis while acknowledging that privacy doctrine cannot specify the remedial architecture the constitutional principle requires (the remand on particularity). Gorsuch proposes a property alternative that reaches the right result for custodial data but cannot explain why government's own databases are constitutionally problematic (the category error). The Government's consent argument fails because modern technology makes meaningful consent structurally impossible (the consent failure). And the duration threshold that the mosaic theory requires cannot be drawn without producing the arbitrary line-drawing the majority rightly rejects (the line-drawing problem).

What connects these failures is the transactional premise they share. Each approach treats the Fourth Amendment as a body of law governing discrete events: a particular search of a particular person's particular data, authorized (or not) by a particular warrant, justified (or not) by particular probable cause. When the constitutional problem is architectural rather than transactional, when it is the existence of the surveillance infrastructure rather than any particular search within it, a transactional framework cannot produce adequate answers. It can extend warrant requirements to new technologies, as *Chatrie* does. It can impose probable cause and particularity

constraints on individual warrants, as the Fourth Circuit will attempt on remand. What it cannot do is address the prior question: whether the surveillance architecture itself, the integrated databases, the centralized repositories, the comprehensive and continuously updated records of citizens' locations, associations, transactions, and activities, is constitutionally permissible.

The fiduciary framework addresses that prior question. The next Part explains how.

PART IV. THE FIDUCIARY ALTERNATIVE

The doctrinal instabilities *Chatrie* exposes share a common source: the transactional premise that the Fourth Amendment governs discrete search events rather than the governmental relationships that produce them. This Part presents an alternative account. The government-citizen information relationship is fiduciary in character, generating categorical constitutional obligations that inhere in the relationship's structure rather than arising from any particular search or seizure. This fiduciary framework resolves each of the instabilities identified in Part III, accommodates the competing doctrinal approaches the *Chatrie* opinions advance, and provides the structural foundation on which the architectural remedies discussed in Part V can rest.⁸²

A. Facts as unownable commons requiring stewardship

The fiduciary framework begins with a premise about the nature of personal information that distinguishes it from both the property model Justice Gorsuch advances and the privacy model the majority employs. Facts about individuals, the places they go, the transactions they conduct, the associations they maintain, are features of the world. They exist independent of any recording and prior to any observation. They are discovered, not created.⁸³

This premise has a direct consequence: facts about individuals cannot be owned. They can be recorded, and records can be held in various custodial arrangements. But the underlying facts belong to no one because they are not the product of anyone's effort or authorship. They are, in the language of trust law, part of the commons: the shared epistemic resources from which all participants in a society draw and to which all contribute.⁸⁴

The commons framing is not merely a theoretical refinement. It has operational implications that the property and privacy models lack. If facts are property, they can be bought, sold, and alienated, and the constitutional protections attending them can be contracted away. If facts are the subject of privacy expectations, those expectations can be deemed unreasonable when social practices shift, as the third-party doctrine demonstrates. But if facts are commons, they cannot be owned, and the obligations attending their custody arise from the custodial relationship rather than from the nature of the thing held. A custodian of commons resources holds them in trust. She may use them for authorized purposes, but she may not appropriate them, repurpose them beyond her authorization, or treat them as her own.

This is the framework's answer to the category error that Part III identified in the property model. The government's own integrated databases, populated through mandatory administrative processes rather than voluntary custodial entrustment, hold facts about citizens that are no less part of the commons than the facts Location History records. The constitutional obligation attaches to the custodial relationship, not to the chain of custody. Whether the government obtains facts about a citizen through a geofence warrant directed to Google, through a tax return the citizen is legally required to file, or through a license application the citizen must submit to drive a car, the government's relationship to those facts is the same: it holds them in a custodial capacity that generates fiduciary obligations.

B. The bilateral trust structure

The commons premise generates a specific relational architecture. Citizens are the natural primary trustees of facts about themselves. They possess those facts by virtue of living their lives. They disclose them, voluntarily or under compulsion, to government and to private entities for specific purposes. Government receives bounded authority to verify and use those facts for constitutionally authorized purposes: collecting taxes, delivering services, enforcing laws, administering regulatory programs.

This relationship exhibits the three structural conditions that fiduciary law has long recognized as generating mandatory fiduciary obligations. First, entrustment: citizens must provide government with information affecting their most fundamental interests, including their liberty, their property, their access to public services, and their participation in civic life.⁸⁵ Second, power asymmetry and mandatory participation: citizens cannot negotiate the terms on which government holds their information, cannot monitor government's use of it, and cannot exit the relationship regardless of dissatisfaction with government's information practices.⁸⁶ Third, inadequacy of contractual or market constraints: the government-citizen relationship is not voluntary, is not governed by arms-length bargaining, and cannot be adequately regulated through the mechanisms (disclosure requirements, consent protocols, market competition) that constrain private custodial relationships.⁸⁷

When these three conditions are present, fiduciary law imposes duties not because the parties bargained for them but because the relationship's structure makes contractual specification inadequate to protect the vulnerable party's interests. As Frankel established, the fiduciary obligation is categorical rather than contractual: it arises from what the relationship is, not from what the parties agreed it would be.⁸⁸ The government-citizen information relationship satisfies all three structural conditions with particular force, precisely because the relationship is sovereign rather than market-derived, is backed by coercive enforcement authority, and cannot be terminated by the citizen.

The *Chatrle* majority approaches this structural analysis without reaching it. The Court's observation that Location History information "is not truly 'shared' as one normally understands the term" because cell phones are "indispensable to participation in modern society" identifies the practical compulsion that makes the government-citizen information relationship non-voluntary.⁸⁹ But the majority frames non-voluntariness as a reason to exempt Location History from the third-party doctrine rather than as evidence of the fiduciary character of the custodial relationship. The framework takes the next step: the structural conditions that make the third-party doctrine inapplicable are the same conditions that generate fiduciary obligations.

C. Four fiduciary duties derived from the Fourth Amendment

The fiduciary character of the government-citizen information relationship generates specific constitutional duties. These duties are not invented by the framework. They are derived from the Fourth Amendment's text, read in light of its structural purposes and the fiduciary principles that inform them.⁹⁰

The duty of loyalty derives from the particularity requirement. The Fourth Amendment's command that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized" is, at its core, a prohibition on repurposing. Information collected for one constitutionally authorized purpose may not be used for another without independent constitutional authorization. When a benefits agency collects a recipient's address for service delivery and shares it with immigration enforcement, it violates the same structural principle as a trustee who diverts trust assets to unauthorized uses. The duty of loyalty requires that each governmental use of citizen information satisfy the particularity requirement independently.

Chatrle illustrates both the duty's necessity and its absence. Justice Jackson's concurrence demonstrates that the geofence warrant's multi-step structure permitted officers to expand the search's scope at steps two and three without returning to the magistrate for purpose-specific authorization, giving them what Jackson called "a 'roving commission' to collect more data absent any justification."⁹¹ The duty of loyalty would require that each expansion satisfy its own particularity and probable cause requirements, a structural constraint the warrant failed to provide and a private corporation had to improvise.

The duty of care derives from the reasonableness standard. The Fourth Amendment prohibits "unreasonable" searches and seizures, a standard that in the fiduciary context requires government to collect only what is necessary for the authorized purpose, to verify facts without retaining the underlying data where retention is not required, and to minimize both the scope and the duration of data holdings. The duty of care is the constitutional expression of the data minimization principle, but it derives its authority from the Fourth Amendment's text rather than from statutory privacy frameworks that lack constitutional force.

The *Chatrle* majority's emphasis on Location History's extraordinary granularity, its twenty-meter precision, its two-minute recording intervals, its capacity to identify which floor of a building a phone occupies, illuminates what the duty of care prohibits.⁹² The constitutional question is not whether this level of precision is useful for law enforcement (it plainly is) but whether it is necessary for the purpose the warrant authorizes. The duty of care requires that government's data collection be calibrated to its constitutional authorization, not to its technological capability.

The duty of confidentiality derives from the search prohibition itself. The Fourth Amendment declares that the right of the people to be secure against unreasonable searches "shall not be violated." In the fiduciary framework, unauthorized access to citizen information is a search, and integrated database architecture that creates the capacity for unauthorized access is itself the constitutional violation, because it establishes the standing, comprehensive, discretionary surveillance authority the Amendment was ratified to prohibit.

This is the duty that connects most directly to the majority's "virtual panopticon" passage. The constitutional wrong, in the majority's formulation, is that "the government can access all of a cell-phone user's movements," that it "possesses" the panopticon.⁹³ The duty of confidentiality translates this insight into an architectural mandate: government information systems must be designed so that unauthorized access is architecturally impossible, not merely procedurally prohibited. Part V develops this mandate in operational terms.

The duty of transparency derives from the warrant requirement. The Fourth Amendment's insistence on warrants issued by neutral magistrates, supported by oath or affirmation, is a transparency mechanism: it requires that government's informational intrusions be visible to an independent authority and, ultimately, to the citizen whose information is accessed. The duty of transparency requires that citizens, as the principals in the fiduciary relationship, be able to know when and how government accesses their information.

The geofence warrant's multi-step structure, in which the magistrate authorized a process whose subsequent stages operated beyond magisterial oversight, violates the duty of transparency.

Jackson's observation that "officers conducted key portions of the search outside the supervision of 'a neutral and detached magistrate'" is a transparency failure as much as a particularity failure.⁹⁴ The two duties are complementary: particularity ensures that each search is authorized for a specific purpose; transparency ensures that the authorization is visible and accountable.

D. Resolving *Chatrle*'s doctrinal instabilities

The fiduciary framework resolves each of the four instabilities Part III identified, because it replaces the transactional premises those instabilities share with a structural account of the governmental relationship.

The duration problem disappears. The constitutional wrong is the surveillance architecture, not the duration of any particular access. The majority's "virtual panopticon" insight is correct: the government "possesses" the surveillance capability regardless of whether it exercises it for two hours or two years. The fiduciary framework explains why this is so. A fiduciary who maintains the capacity to breach her duties has already violated the duty of confidentiality, even if she has not yet accessed the information. The architectural violation is prior to and independent of any transactional search.⁹⁵

The third-party problem disappears. The fiduciary obligation runs between government and citizen, not between government and the custodian through which government obtains information. Whether the government acquires Location History from Google, purchases commercial data broker records, or queries its own integrated databases, its fiduciary obligations to the citizen whose facts it accesses are the same. The custodial chain is irrelevant to the constitutional analysis because the constitutional duty arises from the governmental relationship, not from the mode of acquisition.

The line-drawing problem disappears. The four-factor Otis test asks a structural question, does this governmental information architecture exhibit discretionary power, comprehensive scope, standing authorization, and accountability evasion, rather than a quantitative one about how much aggregation is too much. The test produces determinate answers because it evaluates the

architecture of surveillance authority rather than the output of particular surveillance events. An integrated government database that permits any credentialed official to query comprehensive records of citizens' locations, associations, and transactions, without prior individualized authorization and without citizen notification, exhibits all four Otis characteristics and is constitutionally prohibited regardless of how much data any particular query retrieves.⁹⁶

The property/privacy tension disappears. The fiduciary framework accommodates both approaches because it recognizes the individual as primary trustee of facts about herself, a relationship that generates both the custodial interest Justice Gorsuch identifies (Location History is his "effect" because he holds it in a capacity that generates rights and obligations) and the structural constitutional obligation the majority intuitively feels (the surveillance capability threatens the relationship between government and citizen that the Fourth Amendment was designed to protect). The two analyses are not competing accounts of the same phenomenon; they are complementary descriptions of different dimensions of a single fiduciary relationship.

E. Accommodating Gorsuch: the custodial interest and the trust law resolution

Part II introduced the productive tension between Gorsuch's property analysis and the framework's commonsense premise, and it identified the inalienability problem as the property model's most significant structural vulnerability. This Section completes the resolution.

Gorsuch is correct that Chatrue's Location History data is constitutionally protected, and he is correct that the protection extends even though a third party stores it. His valet analogy captures a genuine structural feature of the relationship: entrusting your property to another for specific purposes does not extinguish your interest in it.⁹⁷ What the analogy also captures, though Gorsuch does not develop the point, is that the entrustment creates a relational obligation. The valet must return the car. He must not use it for unauthorized purposes. He must exercise reasonable care. These obligations arise from the structure of the bailment, not from the terms of any contract, and they cannot be waived by the car's owner because the legal system imposes them categorically on custodial relationships of this type.

The fiduciary framework extends this relational logic to the government-citizen information relationship. The citizen's custodial interest in her data records (Gorsuch's "effects") coexists with, and is completed by, the fiduciary obligations her relationship to government generates. She holds facts about herself as primary trustee; government holds them as secondary fiduciary. The trust law authorities identified in Part II establish that this custodial relationship is inalienable: the citizen cannot contractually extinguish the fiduciary obligations that attend it, any more than a beneficiary can waive the protections of a spendthrift trust.⁹⁸

This resolution preserves what is correct in Gorsuch's analysis (the individual has a constitutionally cognizable interest in data records held by third parties) while avoiding what is problematic (the implication that data-as-property can be alienated through terms of service, and the inability to reach government's own databases). It also explains the majority's intuition that Location History, emails, photographs, and calendar entries stored on Google's servers remain "the individual's own" even though a third party holds them.⁹⁹ They are his own not because he has a property interest in the bits stored on Google's servers, but because his relationship to the facts those records memorialize is custodial, and the obligations attending that custodial relationship cannot be transferred to or extinguished by a third party's data practices.

The fiduciary account thus provides the "coherence" Gorsuch seeks in Fourth Amendment jurisprudence, but it locates that coherence in the structure of the governmental relationship rather than in the property law categories Gorsuch proposes.¹⁰⁰ Both the majority and the concurrence are moving toward the same structural reality. The fiduciary framework names it.

PART V. FROM DOCTRINE TO ARCHITECTURE

The fiduciary framework's constitutional analysis, developed in Part IV, generates specific architectural mandates. These mandates translate the four fiduciary duties into operational requirements for government information systems: requirements that legislatures can enact, that executive agencies can implement, and that courts can enforce through structural injunctions. This

Part identifies three architectural principles that connect the constitutional analysis to the legislative framework discussed in Part VI.¹⁰¹

A. Mandatory sequestration

The duty of confidentiality, as derived from the Fourth Amendment's search prohibition, requires that government information systems be designed so that unauthorized cross-purpose access is architecturally impossible rather than merely procedurally prohibited. The operational expression of this requirement is mandatory sequestration: purpose-limited data stores that architecturally prevent information collected for one constitutionally authorized purpose from being accessed for another without independent constitutional authorization.¹⁰²

Mandatory sequestration is not data siloing in the conventional information-technology sense. It does not require that government agencies maintain wholly separate systems incapable of interoperating. It requires that interoperation occur only through constitutionally compliant channels: queries that are authorized for a specific purpose, that retrieve only the information necessary for that purpose, and that generate auditable records of the access. The distinction is between an integrated database that permits any credentialed official to browse comprehensive records at will, which exhibits the general warrant characteristics the Fourth Amendment prohibits, and a federated architecture that permits authorized queries across purpose-limited stores under conditions of specificity, necessity, and accountability.

Chatrle illustrates both why mandatory sequestration is necessary and what happens in its absence. Google's Location History database was a centralized repository storing comprehensive, continuously updated, precisely geolocated records for over 500 million users worldwide.¹⁰³ The geofence warrant directed to that repository returned data on nineteen individuals, the vast majority of whom had no connection to the crime under investigation. Justice Jackson's concurrence documented that the officers initially sought unbounded data on all nineteen, narrowing only because Google insisted.¹⁰⁴ The warrant's multi-step structure was a procedural attempt at sequestration: anonymized data at step one, narrowed data at step two, identified data at step three.

Jackson demonstrated that the procedural structure failed because the warrant provided no architectural constraint on the officers' discretion at each stage.¹⁰⁵

Mandatory sequestration provides the architectural constraint the warrant could not. Under a sequestration mandate, the Location History database would not exist in the form the geofence warrant exploited, because comprehensive, centralized, continuously updated location records would be architecturally prohibited. Location data would be stored in purpose-limited configurations accessible only through queries satisfying the specificity, necessity, and accountability requirements the fiduciary duties impose.

B. Query-without-collection

The duty of care requires that government collect only what is necessary for the authorized purpose and verify facts without retaining the underlying data where retention is not required. The architectural expression of this requirement is the query-without-collection principle: the proposition that verification does not require retention.¹⁰⁶

The principle is not aspirational. It describes an architecture already deployed at scale. In July 2025, Google migrated Location History from centralized cloud storage to individual users' devices.¹⁰⁷ The majority acknowledged this change in footnote 3; Justice Alito characterized the geofence procedure as "now-obsolete" as a result.¹⁰⁸ Google's migration demonstrates that the world's largest data company, managing location records for hundreds of millions of users, determined that device-level storage was operationally viable and commercially preferable. The company did voluntarily what the fiduciary framework would constitutionally mandate.

Google's architectural shift is not an isolated case. The framework's query-without-collection principle aligns with the technical trajectory of the identity and data governance standards the federal government itself has endorsed. NIST Special Publication 800-63-4, the federal digital identity guideline, recognizes selective disclosure and privacy-enhancing technologies as components of identity assurance architecture.¹⁰⁹ The W3C Verifiable Credentials standard enables cryptographic verification of specific attributes (age, licensure status, benefit

eligibility) without disclosing the underlying data or retaining a record of the verification.¹¹⁰ Zero Trust architecture, now mandated for federal agencies under Executive Order 14028, operates on the principle that every access request must be independently authenticated and authorized rather than trusted on the basis of network position or credential scope.¹¹¹

The fiduciary framework's relationship to these technical standards is complementary rather than competitive. The framework mandates the strongest architecture these standards recognize and adds the legal and constitutional superstructure they cannot provide. NIST can specify technical protocols for privacy-preserving verification. It cannot impose fiduciary duties on government custodians of citizen data, create private rights of action for architectural violations, or establish the constitutional foundation on which judicial enforcement of architectural mandates can rest. The framework provides the constitutional "why" that gives the technical "how" its legal force.¹¹²

C. Structural remedies and judicial enforcement

The fiduciary framework's architectural mandates are enforceable through structural injunctions, the established judicial mechanism for requiring systemic institutional changes when constitutional violations are systemic and architectural. The authority of federal courts to issue structural injunctions requiring comprehensive reform of unconstitutional institutional practices is well established across multiple domains: prison conditions in *Brown v. Plata*, school desegregation in *Swann v. Charlotte-Mecklenburg Board of Education* and *Missouri v. Jenkins*, and institutional mental health care in a line of cases following *Wyatt v. Stickney*.¹¹³

Understanding the structural injunction's role requires distinguishing two levels of constitutional remedy. *Chatrpie's* remand to the Fourth Circuit calls for a warrant-level remedy: the court will evaluate whether this particular warrant satisfied the Fourth Amendment's requirements of particularity and probable cause at each stage of the search process. A warrant-level remedy governs the validity of individual search authorizations. It asks whether the officers' search was constitutional. A structural injunction operates at a different level. It addresses the information

architecture that made the search possible, requiring that the architecture itself satisfy constitutional standards so that the conditions producing the warrant's deficiencies cannot recur. The architectural-level remedy asks whether the system that enabled the search is constitutionally permissible.¹¹⁴

The distinction matters because warrant-level remedies are retrospective and case-specific. They can invalidate a particular search and suppress its fruits. They cannot prevent the next warrant from presenting the same structural deficiencies, because the architecture that produces those deficiencies remains in place. Jackson's concurrence illustrates the point: the geofence warrant's particularity failures arose not from the officers' choices but from the architecture of Google's centralized Location History database, which made comprehensive, undifferentiated surveillance of every person within a geographic area technically trivial and procedurally routine.¹¹⁵ A warrant-level remedy addresses the officers' conduct within that architecture. A structural injunction addresses the architecture itself.

The structural injunction in the government database context operates on the same principle that governs structural injunctions in other institutional reform contexts. The court specifies the constitutional requirements the institution must satisfy without mandating particular operational methods for satisfying them. A decree in the database context would not order a state to install a particular software platform or adopt a particular vendor's architecture. It would require that, within a specified implementation period, the state's information systems satisfy determinate constitutional standards: that no single query or credential permit access to records maintained for distinct statutory purposes without independent authorization specific to the secondary purpose; that verification functions operate through query-without-collection protocols that confirm attributes without retaining the underlying data; that every access to citizen information generate an auditable log entry accessible to the data subject; and that cross-purpose access require individualized authorization documented by the authorizing official and subject to after-the-fact review.¹¹⁶ The state retains full discretion over which technical protocols, system architectures, and implementation timelines satisfy those standards.

This approach preserves judicial restraint while ensuring constitutional compliance. The institutional-competence objection, that courts lack the technical expertise to design government information systems, dissolves because the framework does not require courts to design systems. It requires them to enforce constitutional standards whose content is specified by the fiduciary duties the Fourth Amendment generates. Courts enforce architectural standards in the structural injunction context routinely: they require that prisons provide adequate medical care without specifying which medications to stock; they require that schools achieve unitary status without specifying which bus routes to operate. The fiduciary framework asks courts to do for government databases what they have done for prisons and schools: identify the constitutional violation, specify the structural requirements compliance demands, and monitor institutional progress toward satisfaction of those requirements.¹¹⁷

Structural injunctions and model legislation are complements, not alternatives. The model statutes discussed in Part VI provide fiduciary architectural standards proactively: a state that enacts them builds constitutional compliance into its information systems by design. Structural injunctions enforce those standards reactively: when a state has not enacted adequate legislation or its systems fail to comply with enacted standards, courts can impose compliance on terms and timelines the state does not control. The optimal outcome, from both a constitutional and an institutional perspective, is legislative enactment. Judicially imposed architectural reform is slower, more expensive, more contentious, and less technically informed than legislatively enacted reform, because courts must rely on adversarial proceedings and special masters rather than the state's own technical expertise. But the availability of the structural injunction remedy gives the legislative project its constitutional urgency. States that do not enact fiduciary data governance standards voluntarily may have them imposed judicially. This is the same dynamic that drove institutional reform in the prison and school desegregation contexts, where the prospect of judicially mandated remedies motivated legislative and executive action that preempted the need for judicial intervention.¹¹⁸

If the framework's constitutional analysis is correct, the Fourth Circuit's particularity analysis on remand is an application of fiduciary principles to warrant procedure, whether or not the court frames it in those terms. Each stage of the geofence warrant must satisfy the duties of loyalty (purpose limitation), care (data minimization), confidentiality (architectural prevention of unauthorized access), and transparency (magisterial oversight and citizen notification). The model statutes provide the legislative framework that would make such warrant-by-warrant adjudication largely unnecessary, by ensuring that the information architecture itself satisfies the constitutional standards before any warrant is sought.

PART VI. STATE LEGISLATIVE PATHWAYS

The fiduciary framework's architectural mandates require legislative enactment. Courts can identify constitutional violations, impose structural injunctions, and enforce compliance. They cannot draft comprehensive statutory frameworks governing the full range of government information practices across executive agencies, law enforcement, regulatory bodies, and human services programs. That legislative project is already underway.

A. Three model statutes as *Chatrie*'s legislative response

The framework comprises three companion model statutes, each addressing a distinct layer of the government-citizen information relationship and each operationalizing the constitutional principles *Chatrie* has now reinforced.¹¹⁹

The Verifiable Identity and Digital Autonomy Act (VIDA) addresses the identity and architectural layer. VIDA establishes that government endorses rather than creates identity, requires selective disclosure capabilities (including age verification without birth date revelation), prohibits surveillance-enabling architecture in identity systems, and mandates interoperability through open standards. VIDA operationalizes the duty of care at the infrastructure level: government identity systems must be designed so that verification does not require the collection or retention of information beyond what the specific verification purpose demands.

The Personal Data Trusteeship Act (PDTA) addresses the data governance and fiduciary duties layer. The PDTA codifies the four fiduciary duties identified in Part IV, establishes mandatory data sequestration, requires query-without-collection architecture for verification functions, creates bilateral audit mechanisms (citizen-accessible logs of governmental access to their information), provides enforcement through both Attorney General action and private rights of action, and mandates open standards to prevent vendor lock-in. The PDTA translates the constitutional analysis this Article develops into enforceable statutory obligations.

The Government Algorithmic Accountability and AI Fiduciary Act (GAAFA) addresses the algorithmic accountability layer. GAAFA operationalizes Justice Jackson's particularity analysis for algorithmic decision-making: when government employs algorithmic processes to select individuals for heightened scrutiny, to determine benefit eligibility, or to allocate enforcement resources, those processes must satisfy the same fiduciary duties that govern human decision-making. Algorithmic systems must be auditable, their criteria must be specified with particularity, and their outputs must be subject to meaningful human review. GAAFA addresses the gap *Chatrle* exposes at the warrant level, where the multi-step geofence protocol delegated narrowing decisions to officers' unguided discretion, and extends it to the full range of algorithmic processes through which government acts on citizen data.

The three statutes are successive layers completing a single architecture. VIDA governs how identity is established and verified. The PDTA governs how government holds and uses the data identity verification generates. GAAFA governs how algorithmic systems process that data to produce decisions affecting citizens. Together, they provide the comprehensive statutory framework that the constitutional principle *Chatrle* articulates requires but that judicial enforcement alone cannot deliver.

B. Utah as proof of concept

The framework is not theoretical. Elements of VIDA and the PDTA have been enacted in Utah through Senate Bills 260 and 275.¹²⁰ SB 260, enacted in 2025, establishes government

endorsement rather than creation of identity, requires selective disclosure capabilities, and prohibits surveillance-enabling architecture in the state's digital identity system. SB 275, enacted in 2026, codifies fiduciary duties for government handling of personal data, creates a Digital Identity Bill of Rights, requires holder-controlled audit logs, mandates open standards, and provides Attorney General enforcement with private remedies.

These bills incorporate elements of the framework's model statutes. They do not constitute full enactment. SB 260 does not mandate query-without-collection architecture across all state information systems. SB 275 does not require mandatory sequestration of purpose-limited data stores. Neither bill addresses algorithmic accountability. The Utah enactments are a foundation, not a completed structure. They demonstrate that the framework's core concepts, government endorsement of identity, fiduciary duties for data stewardship, citizen-accessible audit mechanisms, are legislatively viable and can survive the political process that produces enacted law.

The framework's legislative viability extends beyond Utah. Multiple additional states are in substantive exploration and engagement through the Secure Electronic Digital Identity (SEDI) Consortium, a multistate initiative addressing identity verification architecture.¹²¹ The SEDI Consortium addresses the identity layer that VIDA governs. The full Fiduciary Commons Framework adds the enforceable fiduciary legal relationship (the PDTA) and the algorithmic accountability layer (GAAFA) that SEDI's identity-focused architecture does not reach. The relationship between SEDI and the framework is successive rather than competitive: SEDI addresses how identity is verified; the framework adds the constitutional and legal superstructure governing what government may do with the information identity verification generates.

C. State leadership as the practical path

State legislative action is not a second-best alternative to federal legislation. It is the constitutionally appropriate path for three independent reasons.

First, federal digital privacy legislation remains stalled. Congress has not enacted comprehensive privacy legislation despite decades of advocacy. The federal impasse is structural rather than contingent: the competing interests of law enforcement, technology companies, federal agencies, and privacy advocates have prevented consensus on the scope, enforcement mechanisms, and preemptive effect of any federal framework. State legislatures face narrower versions of these political dynamics, and several have demonstrated the capacity to act. Utah's enactment of framework elements confirms that the political conditions for legislative progress exist at the state level even when they do not exist at the federal level.¹²²

Second, state constitutions provide independent privacy foundations. Many state constitutions contain explicit privacy provisions that go beyond the Fourth Amendment's text. These provisions provide independent constitutional authority for state legislatures to impose fiduciary obligations on government information practices, authority that does not depend on federal Fourth Amendment doctrine and cannot be preempted by federal legislation that falls short of the constitutional floor.¹²³

Third, *Chatrle*'s remand creates a window for state legislative action. The Fourth Circuit must now evaluate the geofence warrant's compliance with particularity and probable cause requirements. Whatever standards the court articulates will guide law enforcement practices in the Fourth Circuit. State legislatures that enact the framework's architectural standards before those judicial standards crystallize position their states as constitutional leaders rather than respondents to judicially imposed requirements. The model statutes provide the architectural standards the courts will eventually need to evaluate: by enacting them proactively, state legislatures establish the constitutional framework rather than reacting to it.

PART VII. CONCLUSION

Chatrle v. United States is the most significant Fourth Amendment decision bearing on government surveillance architecture since *Carpenter*. The majority's identification of the "virtual

panopticon," its categorical rejection of durational thresholds, and its further erosion of the third-party doctrine collectively establish that the Fourth Amendment's protections extend to the surveillance capability itself, not merely to its exercise in any particular case. Justice Jackson's concurrence demonstrates that the geofence warrant's particularity failures are structural rather than incidental, arising from the interaction between an insufficiently constrained warrant and a centralized database architecture that made comprehensive, undifferentiated surveillance technically trivial. Justice Gorsuch's property-based concurrence reaches the correct result through an alternative doctrinal pathway that illuminates, even as it cannot fully resolve, the constitutional relationship between individuals and their data.

But *Chatrre* also demonstrates, with equal clarity, the limits of judicial enforcement. The Court can declare that accessing Location History is a search. It can impose a warrant requirement. It can remand for particularity and probable cause analysis. What it cannot do is mandate the architectural redesign of government information systems that the constitutional principle it has articulated requires. The remand to the Fourth Circuit will produce a holding about this warrant, applied to this technology, in this case. It will not produce the comprehensive architectural standards governing how government collects, holds, queries, shares, and disposes of citizen data across the full range of administrative, regulatory, and law enforcement functions.

This is not a criticism of the Court. It is a description of institutional competence. The distinction between constitutional interpretation and political implementation is foundational to the American constitutional structure. Courts say what the Constitution requires. Legislatures design the institutional architectures that satisfy those requirements. Executives build and operate the systems those architectures specify. The fiduciary framework respects this division of institutional labor while insisting that the constitutional requirements are non-negotiable.

The framework's central claim is that the government-citizen information relationship is fiduciary in character, generating categorical constitutional obligations derived from the Fourth Amendment's text and structural purposes. This claim is not a policy proposal. It is a constitutional interpretation, subject to the same modes of argument, the same standards of justification, and the

same processes of judicial review as any other claim about what the Constitution requires. The four fiduciary duties the framework identifies, loyalty, care, confidentiality, and transparency, are derived from the Amendment's particularity requirement, its reasonableness standard, its search prohibition, and its warrant requirement. They are not additions to the constitutional text. They are specifications of what the text demands when applied to the architectural realities of government information systems in the digital age.

The architectural mandates that flow from those duties, mandatory sequestration, query-without-collection, bilateral audit mechanisms, individualized cross-purpose authorization, are the operational translation of constitutional requirements into system design principles. They are constitutionally required in the same sense that racially unitary school systems are constitutionally required: not because the Constitution specifies a particular system design, but because the constitutional principle (equal protection, or in this case, security against unreasonable searches) cannot be satisfied without architectural compliance. The model statutes operationalizing these mandates, VIDA, the PDTA, and GAAFA, are the legislative instruments through which states can achieve that compliance proactively rather than waiting for courts to impose it through structural injunctions.

Chatrie vindicates this constitutional analysis at every point where the decision engages the framework's premises. The majority's rejection of durational thresholds confirms that the constitutional violation inheres in the surveillance capability rather than its exercise. The majority's further erosion of the third-party doctrine confirms that consent-based models cannot produce stable constitutional protections in a technologically mediated society. Jackson's "roving commission" analysis confirms that the particularity requirement demands architectural specificity that procedural warrant constraints cannot deliver. And Gorsuch's property analysis, resolved through the trust law inalienability principles the framework supplies, confirms that the individual's custodial relationship to her data generates obligations that transcend both property and privacy doctrine.

At the same time, *Chatrle* demonstrates why judicial enforcement of the Fourth Amendment, however robust, cannot substitute for the architectural governance the model statutes provide. The decision addresses one technology (geofence warrants directed to Location History data), in one context (criminal investigation), through one remedial mechanism (the exclusionary rule, subject to the good-faith exception that will almost certainly save this conviction on remand). The constitutional principle the decision articulates reaches every integrated government database, every cross-agency data sharing agreement, every algorithmic system that processes citizen data to produce governmental decisions. Judicial enforcement through criminal suppression proceedings cannot reach that full domain. Legislative enactment of fiduciary architectural standards can.

The Court has told us that the government possesses a virtual panopticon. It has told us that the Fourth Amendment applies to that panopticon. It has not told us how to dismantle it, because that is not the Court's institutional role. The fiduciary framework provides the constitutional blueprint. The model statutes provide the legislative tools. The states that have begun enacting them demonstrate that the project is operationally viable and politically achievable.

The Court named the panopticon. The framework dismantles it.

ENDNOTES

1. *Chatrie v. United States*, 609 U.S. ___, slip op. at 29 (2026).
2. See *Carpenter v. United States*, 585 U.S. 296, 310 n.3 (2018) (reserving the question whether accessing less than seven days of cell-site location information constitutes a Fourth Amendment search).
3. *Chatrie*, slip op. at 21.
4. *Id.*
5. *Id.* at 30.
6. The Fiduciary Commons Framework is developed at length in three companion articles: Michael G. Leahy, *Digital General Warrants: Why Government Databases Violate the Fourth Amendment* (2026) (available at <https://ssrn.com/abstract=6434318>) [hereinafter Leahy, *Digital General Warrants*] (establishing that integrated government databases reconstitute the general warrant in digital form); Michael G. Leahy, *Government as Information Trustee: A Fiduciary Framework for Surveillance-Age Privacy* (2026) (available at <https://ssrn.com/abstract=6434361>) [hereinafter Leahy, *Information Trustee*] (developing the bilateral trust architecture and the four fiduciary duties constitutional compliance requires); Michael G. Leahy, *Completing the Mosaic: How the Fiduciary Framework Grounds Technology-Centered Fourth Amendment Theory in Enforceable Constitutional Structure* (forthcoming 2026) [hereinafter Leahy, *Completing the Mosaic*] (grounding Professor David Gray's technology-centered Fourth Amendment theory in enforceable constitutional structure). These companion articles were completed in February 2026, before the Supreme Court's decision in *Chatrie*. This Article applies the framework those articles develop to the *Chatrie* decision and its implications for state legislative action.
7. Utah S.B. 260, 2025 Gen. Sess. (Utah 2025) (codified at Utah Code Ann. §§ 63-24-101 to -401) (establishing government endorsement rather than creation of identity, requiring selective disclosure capabilities, and prohibiting surveillance-enabling architecture); Utah S.B. 275, 2026 Gen. Sess. (Utah 2026) (codifying fiduciary duties, creating a Digital Identity Bill of Rights, requiring holder-controlled audit logs, and mandating open standards). These bills incorporate elements of the framework's model statutes but do not constitute full enactment of those statutes.
8. See Leahy, *Digital General Warrants*, *supra* note 6, at Part I.A (deriving the four-factor test from James Otis's 1761 denunciation of the writs of assistance and applying it to demonstrate that federal fusion centers, FBI Criminal Justice Information Services systems, and state integrated databases each exhibit all four characteristics simultaneously).
9. *Chatrie v. United States*, 609 U.S. ___, slip op. at 16-18 (2026).
10. *Id.* at 16-17; *cf. Carpenter v. United States*, 585 U.S. 296, 302, 312 (2018).
11. *Chatrie*, slip op. at 18.
12. *Id.*
13. *Carpenter*, 585 U.S. at 310, n.3.
14. Brief for United States at 12, 20, *Chatrie v. United States*, No. 25-112.
15. *Chatrie*, slip op. at 19 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).
16. *Id.*
17. *Id.* at 20 (quoting *Kyllo v. United States*, 533 U.S. 27, 37 (2001)).
18. *Id.* (quoting *Kyllo*, 533 U.S. at 37).

19. *Id.*; see *Katz v. United States*, 389 U.S. 347, 354 n.14 (1967).
20. *Chatrie*, slip op. at 22 n.10.
21. *Id.* at 21.
22. *Id.*
23. *Carpenter*, 585 U.S. at 309, 315.
24. Brief for United States at 13, 22, *Chatrie*, No. 25-112.
25. *Chatrie*, slip op. at 25-26.
26. *Id.* at 26.
27. *Id.* at 27.
28. *Id.* at 28.
29. *Id.*
30. *Id.* at 30.
31. *Id.* at 30-31.
32. *Id.* at 32.
33. *Id.* at 1-4 (Jackson, J., concurring).
34. *Id.* at 1 (Jackson, J., concurring) (emphasis in original).
35. *Id.* at 2 (Jackson, J., concurring).
36. *Id.* (quoting *Berger v. New York*, 388 U.S. 41, 59 (1967)).
37. *Id.* at 3 (Jackson, J., concurring).
38. *Id.*; see 590 F. Supp. 3d 901, 923 (E.D. Va. 2022).
39. *Chatrie*, slip op. at 3 (Jackson, J., concurring) (quoting *Steagald v. United States*, 451 U.S. 204, 220 (1981)).
40. *Id.* at 1 (Gorsuch, J., concurring in the judgment).
41. *Id.* at 1-3 (Gorsuch, J., concurring in the judgment); see *Carpenter*, 585 U.S. at 391 (Gorsuch, J., dissenting).
42. See *Chatrie*, slip op. at 4 (Gorsuch, J., concurring in the judgment) (characterizing Fourth Amendment jurisprudence as analogous to the Court's obscenity doctrine in the 1960s).
43. *Id.* at 6-7 (Gorsuch, J., concurring in the judgment).
44. *Id.* at 7 (quoting *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 149-50 (2021)).
45. *Id.* at 7-8 (Gorsuch, J., concurring in the judgment) (citing Va. Code Ann. § 18.2-152.2; Tex. Penal Code Ann. § 33.01(16); Ga. Code Ann. § 16-9-93(b), (g)).
46. *People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023).
47. Brief for Cato Institute as *Amicus Curiae* 14-15 & n.5, *Chatrie*, No. 25-112.
48. *Chatrie*, slip op. at 8 (Gorsuch, J., concurring in the judgment) (quoting *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting)).
49. *Id.* at 8-9 (Gorsuch, J., concurring in the judgment).
50. *Id.* at 10 (Gorsuch, J., concurring in the judgment).

51. *Cf. id.* at 8 (Gorsuch, J., concurring in the judgment); *Chatrie*, slip op. at 12 n.6 (majority opinion) (responding that the privacy analysis is not "groping toward" Gorsuch's property framework but reflects the independent influence of property law on "shared societal expectations" of privacy).
52. *Id.* at 8 (Gorsuch, J., concurring in the judgment); Brief for United States at 34-36.
53. Restatement (Third) of Trusts §§ 58-59 (Am. Law Inst. 2003).
54. *Ill. Cent. R.R. Co. v. Illinois*, 146 U.S. 387, 452-53 (1892).
55. Tamar Frankel, *Fiduciary Law*, 71 Calif. L. Rev. 795, 807-18 (1983); Tamar Frankel, *Fiduciary Law* 1-22, 47-60 (Oxford 2d ed. 2010).
56. Robert H. Sitkoff, *An Agency Costs Theory of Trust Law*, 89 Cornell L. Rev. 621, 628-34 (2004).
57. *Chatrie*, slip op. at 11 (majority opinion) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).
58. *Id.* at 1-2 (Alito, J., dissenting).
59. *See id.* at 32 n.5 (majority opinion) (noting that the Fourth Circuit is "free to revisit the exclusionary rule issue in light of our opinion").
60. *Id.* at 1 (Alito, J., dissenting).
61. *Id.* at 4 n.3 (majority opinion).
62. *Id.* at 1 (Alito, J., dissenting).
63. *Id.* at 1-3 (Barrett, J., dissenting).
64. For fuller development of each failure mode, see Michael G. Leahy, *Digital General Warrants: Why Government Databases Violate the Fourth Amendment* (2026), at Part II.A (available at <https://ssrn.com/abstract=6434318>).
65. *See supra* Part II.C (analyzing Gorsuch's concurrence); *Chatrie*, slip op. at 5-10 (Gorsuch, J., concurring in the judgment).
66. *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 347-48 (1991). *Feist* holds that facts cannot be copyrighted because copyright protects only original works of authorship, and facts, "do not owe their origin to an act of authorship." *Id.* at 347. The structural insight, that facts exist independent of human effort and cannot be owned, has implications beyond copyright's doctrinal boundaries.
67. *See* Leahy, *Digital General Warrants*, *supra* note 6, at Part I.C (documenting the scope of federal and state integrated database systems); *see also* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 Harv. L. Rev. 1790 (2022) (documenting post-*Carpenter* doctrinal inconsistency).
68. *See supra* Part II.A.3 (analyzing the majority's treatment of the third-party doctrine).
69. *Chatrie*, slip op. at 25-26.
70. *Id.* at 27.
71. *Id.* at 28.
72. *See* Tamar Frankel, *Fiduciary Law* 47-60 (Oxford 2d ed. 2010) (concluding that mandatory governmental relationships, "precisely because exit is foreclosed and bargaining is impossible, generate categorical fiduciary obligations stronger than those arising in voluntary private relationships").
73. *Chatrie*, slip op. at 28.
74. *United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).
75. *See* W. Bishop, Pew Research Center, Mobile Fact Sheet (Nov. 20, 2025) (91% smartphone ownership), cited in *Chatrie*, slip op. at 2.

76. *Chatrie*, slip op. at 3 (Gorsuch, J., concurring in the judgment) (quoting *Carpenter*, 585 U.S. at 391 (Gorsuch, J., dissenting)).
77. *United States v. Jones*, 565 U.S. 400, 413-14 (2012) (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment); David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 65 (2013).
78. *Chatrie*, slip op. at 19 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
79. *Id.* at 20 (quoting *Kyllo*, 533 U.S. at 37).
80. *Compare* *Leaders of a Beautiful Struggle v. Baltimore City Police Dep't*, 2 F.4th 330 (4th Cir. 2021) (extending *Carpenter* to wide-area aerial surveillance), *with* *United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021), cert. denied, 142 S. Ct. 1107 (2022) (declining to extend *Carpenter* to nineteen months of pole camera surveillance). *See generally* Tokson, *supra* note 67, at 1790.
81. *See* Leahy, *Digital General Warrants*, *supra* note 6, at Part I.A (deriving the four-factor test from Otis's denunciation of writs of assistance); *see also* Michael G. Leahy, *Completing the Mosaic: How the Fiduciary Framework Grounds Technology-Centered Fourth Amendment Theory in Enforceable Constitutional Structure* (forthcoming 2026), at Part II.B (applying the four-factor test to resolve threshold indeterminacy in Professor David Gray's quantitative privacy framework).
82. For the full development of the fiduciary framework, *see* Leahy, *Information Trustee*, *supra* note 6; Leahy, *Digital General Warrants*, *supra* note 6.
83. *See* *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 347-48 (1991); Leahy, *Digital General Warrants*, *supra* note 6, at Part II.B.
84. Leahy, *Information Trustee*, *supra* note 6, at Part II.A.
85. Tamar Frankel, *Fiduciary Law*, 71 Calif. L. Rev. 795, 807-11 (1983) (identifying entrustment of property or power as the first structural condition generating fiduciary obligation).
86. *Id.* at 808-09 (identifying vulnerability arising from power asymmetry and mandatory participation as the second structural condition).
87. *Id.* at 809-11 (identifying inadequacy of market mechanisms or contractual specification as the third structural condition); *see also* Tamar Frankel, *Fiduciary Law* 47-60 (Oxford 2d ed. 2010) (concluding that governmental relationships generate fiduciary obligations with particular force because exit is foreclosed and bargaining is impossible).
88. Frankel, *Fiduciary Law*, 71 Calif. L. Rev. at 814-18 (establishing the categorical rather than contractual character of fiduciary duties).
89. *Carpenter v. United States*, 585 U.S. 296, 315 (2018), quoted in *Chatrie*, slip op. at 25.
90. *See* Leahy, *Information Trustee*, *supra* note 6, at Parts II.D-II.E (deriving the four fiduciary duties from the Fourth Amendment's text and structural purposes).
91. *Chatrie*, slip op. at 2 (Jackson, J., concurring) (quoting *Berger v. New York*, 388 U.S. 41, 59 (1967)).
92. *Id.* at 16-17 (majority opinion).
93. *Id.* at 21.
94. *Id.* at 2 (Jackson, J., concurring) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)).
95. *See* Leahy, *Digital General Warrants*, *supra* note 6, at Part I.D (developing the proposition that the constitutional violation inheres in the surveillance capability rather than its exercise); *cf.* *United States v. Jones*, 565 U.S. 400,

- 416 (2012) (Sotomayor, J., concurring) ("[T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").
96. See Leahy, *Digital General Warrants*, *supra* note 6, at Part I.A (deriving the four-factor test from James Otis's 1761 denunciation of the writs of assistance); Leahy, *Completing the Mosaic*, *supra* note 6, at Part II.B (applying the test to resolve threshold indeterminacy).
 97. *Chatrie*, slip op. at 8 (Gorsuch, J., concurring in the judgment).
 98. See *supra* notes 53-56 and accompanying text (discussing Restatement (Third) of Trusts §§ 58-59, *Illinois Central Railroad Co. v. Illinois*, 146 U.S. 387, 452-53 (1892), Frankel, and Sitkoff).
 99. *Chatrie*, slip op. at 18, 25 (majority opinion).
 100. *Cf. id.* at 8 (Gorsuch, J., concurring in the judgment) (arguing that the majority's privacy analysis produces results more "coheren[t]" with property principles than with the *Katz* framework the majority professes to apply).
 101. For the full architectural treatment, including six implementation scenarios addressing specific objections (emergency medical access, fraud detection, multi-service coordination, guardianship, child welfare, and criminal investigation), see Michael G. Leahy, *Data Lakes Are a Choice, Not a Necessity: How Constitutional Architecture Exposes the Convenience Excuse* (2026) [hereinafter Leahy, *Data Lakes*] (available at <https://ssrn.com/abstract=6212159>), at Parts I-II.
 102. See Leahy, *Data Lakes*, *supra* note 101, at Part I.A (developing the mandatory sequestration principle); Leahy, *Digital General Warrants*, *supra* note 6, at Part III.A.
 103. *Chatrie*, slip op. at 3 (majority opinion).
 104. *Id.* at 3 (Jackson, J., concurring).
 105. *Id.* at 1-3 (Jackson, J., concurring).
 106. See Leahy, *Data Lakes*, *supra* note 101, at Part I.D (developing the query-without-collection principle and demonstrating its operational viability).
 107. See Brief for Google LLC as *Amicus Curiae* 2, *Chatrie*, No. 25-112 (representing that Google "is no longer capable of responding to geofence warrants that seek Location History data" following the migration to device-level storage).
 108. *Chatrie*, slip op. at 4 n.3 (majority opinion); *id.* at 1 (Alito, J., dissenting) (characterizing the geofence procedure as "now-obsolete").
 109. See NIST Special Publication 800-63-4, *Digital Identity Guidelines* (2022).
 110. See W3C, *Verifiable Credentials Data Model v2.0* (2024).
 111. Exec. Order No. 14028, 86 Fed. Reg. 26,633 (May 17, 2021).
 112. See Leahy, *Data Lakes*, *supra* note 101, at Part I.C (developing the "NIST Plus" positioning: the framework mandates the strongest architecture NIST recognizes and adds the legal and constitutional superstructure NIST cannot provide).
 113. *Brown v. Plata*, 563 U.S. 493 (2011); *Swann v. Charlotte-Mecklenburg Bd. of Educ.*, 402 U.S. 1 (1971); *Missouri v. Jenkins*, 495 U.S. 33 (1990); *Missouri v. Jenkins*, 515 U.S. 70 (1995); *Wyatt v. Stickney*, 325 F. Supp. 781 (M.D. Ala. 1971), *aff'd* in relevant part sub nom. *Wyatt v. Aderholt*, 503 F.2d 1305 (5th Cir. 1974). See generally Leahy, *Digital General Warrants*, *supra* note 6, at Part III.C (surveying structural injunction authority across institutional contexts and applying it to the government database context).

114. See Leahy, *Data Lakes*, *supra* note 101, at Part III (developing the phased implementation timeline and the principle that structural injunctions specify constitutional requirements without mandating particular technical implementations).
115. See *Chatrue*, slip op. at 1-3 (Jackson, J., concurring) (documenting that the warrant's particularity deficiencies arose from the interaction between the warrant's multi-step structure and the architecture of Google's centralized Location History database).
116. These requirements illustrate the decree's register and specificity. For the full architectural specification, including phased implementation timelines and compliance monitoring protocols, see Leahy, *Data Lakes*, *supra* note 101, at Part III.
117. Cf. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004) (arguing that courts should defer to legislatures on surveillance policy). The fiduciary framework answers Kerr's institutional-competence concern directly: courts enforce constitutional standards; legislatures design implementation architectures satisfying those standards. The division of institutional labor Kerr advocates is precisely what the framework provides.
118. See, e.g., Malcolm M. Feeley & Edward L. Rubin, *Judicial Policy Making and the Modern State: How the Courts Reformed America's Prisons* 13-46 (1998) (documenting how structural injunction litigation in the prison context motivated legislative and executive reform that preempted judicially imposed remedies in states that acted proactively).
119. The model statutes are available at fiduciarycommons.com. For the full legislative text with commentary, see Leahy, *Data Lakes*, *supra* note 101, at Appendices A-B.
120. Utah S.B. 260, 2025 Gen. Sess. (Utah 2025) (codified at Utah Code Ann. §§ 63-24-101 to -401); Utah S.B. 275, 2026 Gen. Sess. (Utah 2026).
121. See SEDI Consortium, <https://sediconsortium.org> (documenting multistate exploration and engagement with identity verification architecture).
122. See Leahy, *Data Lakes*, *supra* note 101, at Part III.A (analyzing state leadership as the practical path for fiduciary data governance legislation, and documenting the federal legislative impasse).
123. See, e.g., Cal. Const. art. I, § 1 (enumerating privacy as an inalienable right); Mont. Const. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").