

THE GOVERNMENT'S POWER TO KNOW

Fiduciary Commons, Ordered Informational Authority, and the Architecture of Limited Government

Michael G. Leahy

September 2026 | Publication 2.1 | Fiduciary Commons Government Information Architecture Standard (FCGIAS) Version 2.2 Candidate Standard with IR-01 Controlled Clarification

ABSTRACT

Modern government can acquire broad power to know without creating a single centralized database. Interoperability, shared query, commercial enrichment, correlation, inference, digital identity, and artificial intelligence can combine otherwise lawful systems into standing informational capability that no individual office was separately authorized to possess. This paper develops Fiduciary Commons as a theory of legitimate informational relationships and Ordered Informational Authority (OIA) as a theory of governmental power to obtain, verify, know, correlate, infer, disclose, retain, and act upon information. Publication 2.1 incorporates the Version 2.2 distinction between Positive Legal Authority and Legitimate Informational Authority and the IR-01 clarification that legitimate authority is an outer ceiling, not a specification for ordinary standing capability. The resulting architecture applies two constraints: Standing Technical Informational Capability should not materially exceed Necessary Standing Informational Capability, and Necessary Standing Informational Capability must remain within Standing Legitimate Informational Authority. The paper traces this mature rule to an earlier design frame, Utility, Security, and Autonomy, in which No Phone Home and least disclosure already treated unnecessary surveillance capability as an architectural defect. The framework therefore does not maximize privacy against government. It seeks limited informational government: sufficient capability for legitimate public functions, with materially broader power becoming available when both legitimate authority and functional necessity expand.

Keywords: Fiduciary Commons; Ordered Informational Authority; Authority-Capability Correspondence Principle; Necessary Standing Informational Capability; Structural Least Power; Fiduciary Commons Government Information Architecture Standard (FCGIAS); government information architecture; limited government; decentralization; digital identity; artificial intelligence; procurement.

INTRODUCTION: THE ARCHITECTURE OF GOVERNMENTAL KNOWLEDGE

Imagine a state government in which every agency follows the rules assigned to it. The motor vehicle agency lawfully maintains licensing records. The tax agency lawfully maintains tax records. The health department protects the records entrusted to it. Human-services programs maintain eligibility files under their governing statutes. The information-security office enforces strong authentication, encryption, logging, and role-based access. Contractors comply with their contracts. No employee steals a password, exceeds an assigned permission, or sells information. No database is breached.

Now add interoperability. Agencies can resolve identities across systems. A shared service can query records without copying them into a new repository. Commercial data can be acquired through a subscription. An analytics layer can correlate transactions across programs. An artificial-intelligence agent can call multiple authorized interfaces, infer relationships, and recommend action. A fraud unit can search for patterns that no single agency could see. A citizen-service portal can assemble a cross-program picture in order to make government easier to navigate. Nothing in this description necessarily requires a traditional data lake. Nothing necessarily requires misconduct.

Yet the resulting government may possess something none of the component statutes, databases, or offices separately created: a standing capacity to construct a materially comprehensive account of an individual's life across purposes. The important question is therefore not exhausted by asking whether each record was collected lawfully, whether each database is secure, or whether each official has a legitimate job. It is also necessary to ask what informational power the architecture has created for government as an institution.

That is the problem this paper addresses. Modern information governance is rich in rules governing collection, access, use, disclosure, retention, security, and individual rights. Those rules matter. They are indispensable. But they often begin after a more basic institutional choice has already been made: what information systems government will build, connect, subscribe to, or make computationally available. Once a standing capability exists, ordinary governance frequently concentrates on whether a particular official used it properly. The prior question has two parts: whether the capability remains within the governmental informational authority legitimately available without further authorization, and whether ordinary standing capability materially exceeds what is reasonably necessary to perform the legitimate standing function.

The distinction matters because capability is power. A government that can reconstruct movements, resolve identities, correlate benefits and tax records, infer relationships, enrich public records with commercial data, and direct AI across those sources possesses a form of institutional power even before a particular official chooses a target. The power may be used lawfully. It may be valuable. It may sometimes be expressly authorized. But its existence should not be confused with its legitimacy.

The Supreme Court's 2026 decision in *Chatrie v. United States* brings the problem into unusually sharp focus. The Court held that police conduct a Fourth Amendment search when they gain access to a person's Google Location History, even for a limited period and even though the information is held by a third-party technology company. In explaining why, the majority did not treat the short interval ultimately reviewed as dispositive. It looked to the capacity of the Location History system to expose movements at scale and described the government's access in terms of a "virtual panopticon." The Court nevertheless stopped where adjudication ordinarily stops. It remanded questions of probable cause and particularity at the stages of the geofence process. It did not decide whether the surveillance infrastructure that makes such searches possible is independently unconstitutional.

That distinction should be preserved. *Chatrie* does not hold that standing surveillance architecture is itself a completed Fourth Amendment violation. But it makes the capability of the surveillance instrument constitutionally salient. Fiduciary Commons takes the next question seriously: if constitutional concern can turn on the capacity of a digital system to reveal a person's life, what principles should govern the architecture through which government acquires and exercises informational power before a particular search, query, correlation, or inference occurs?¹

The same problem appears outside criminal investigation. A benefits system can create a population-scale profile in the name of seamless service. A digital-identity system can minimize the attributes shown to a verifier while allowing an issuer or identity provider to observe every presentation. A fraud system can turn a legitimate program-integrity mission into a permanent cross-government query fabric. An AI layer can reconstruct functional centralization over physically distributed databases. In each case, the decisive architectural question is not where the bytes reside. It is what government can know, through what standing authority, and what must occur before government can know materially more.

Fiduciary Commons begins from a proposition about limited government. Governmental authority is delegated rather than inherent and unlimited. American constitutional thought has long described public

¹ *Chatrie v. United States*, 609 U.S. ___, No. 25-112, slip op. at 10-29 (June 29, 2026). The Court held that officers conduct a Fourth Amendment search when they access a person's Google Location History, even for a limited period and when the data is obtained from a third-party technology company.

power through the language of delegation, public trust, accountability, particular purposes, and divided authority. Fiduciary Commons argues that informational authority is one species of that delegated governmental power. Government therefore should not acquire generalized informational authority merely because records exist, technology permits access, a vendor offers a capability, or an administrative objective would be easier to achieve with broader knowledge.

This is not a claim that privacy should always defeat administration, security, fraud prevention, public health, or law enforcement. Nor is it an argument for informationally weak government. The framework's objective is ordered power. Government should be capable of knowing what it is legitimately authorized to know, when that knowledge is necessary to perform a lawful function, with sufficient confidence to act. But materially broader power to know should arise because legitimate authority has materially expanded, not because a system quietly accumulated reusable access.

The general theory proposed here is Ordered Informational Authority, or OIA. OIA concerns the allocation of power to obtain, verify, know, correlate, infer, disclose, retain, and act upon information among persons, institutions, programs, and governments according to legitimate relationships, purposes, jurisdiction, and authority. Fiduciary Commons is the constitutional and fiduciary governance model that applies OIA to governmental information concerning persons. FCGIAS is the technical and institutional architecture designed to make those limits inspectable and enforceable.

The architecture follows a simple but demanding rule, the Authority-Capability Correspondence Principle, or ACCP. After the IR-01 clarification, ACCP operates through two nested constraints: government's Standing Technical Informational Capability should correspond to, and not materially exceed, its Necessary Standing Informational Capability; Necessary Standing Informational Capability, in turn, must remain within Standing Legitimate Informational Authority. Authority is therefore a ceiling, not a procurement specification. A government may possess legitimate authority to obtain additional information when defined future conditions arise without needing to maintain the entire outer boundary of that authority as ordinary standing power. The architecture must be capable of expanding when emergencies arise, investigations develop, fraud predicates mature, courts issue orders, legislatures create programs, or individuals request services. But materially broader capability should follow a transition in which both legitimate authority and the necessity for that capability have materially expanded.²³

Figure 1 summarizes the Version 2.2 architecture after IR-01. Delegated public authority and legitimate governmental function supply the institutional starting point. Positive Legal Authority identifies a competent legal source, while Originating Informational Purpose and Informational Justification help determine Standing Legitimate Informational Authority. The new intermediate layer, Necessary Standing Informational Capability, asks how much of that outer authority boundary must actually remain available as ordinary standing power. Structural Least Power and Least Informational Power constrain that layer. ACCP then compares Necessary Standing Informational Capability with deployed Standing Technical Informational Capability. For citizen-originated interactions, the individual's specific purpose leads toward a necessary governmental question, Authorized Answer, No Phone Home or functional decentralization, and the least informationally powerful capability reasonably sufficient for the function.

2 FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD VERSION 2.2, IR-01 Adoption and Freeze Update §§ 3-9 (Sept. 11, 2026); FC-P2.2-IR01, Narrow Verification §§ III-VI (Sept. 11, 2026). IR-01 passed narrow verification with no Priority 1 or Priority 2 contradiction and clarifies the relation as Standing Technical Informational Capability <= Necessary Standing Informational Capability <= Standing Legitimate Informational Authority.

3 FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD VERSION 2.1, Candidate Standard, §§ 18-20, 28, 93-99 (2026) [hereinafter FCGIAS 2.1]. Version 2.1 established the Authority-Capability Correspondence Principle and the distinction between standing technical capability and informational authority. The current rule is FCGIAS Version 2.2, Consolidated Controlling Edition, incorporating IR-01, under which Standing Technical Informational Capability must not materially exceed Necessary Standing Informational Capability, which must remain within Standing Legitimate Informational Authority.

Figure 1. Version 2.2 Architecture After IR-01

Authority is a ceiling, not a procurement specification. Ordinary standing capability is limited by necessity within legitimate authority.

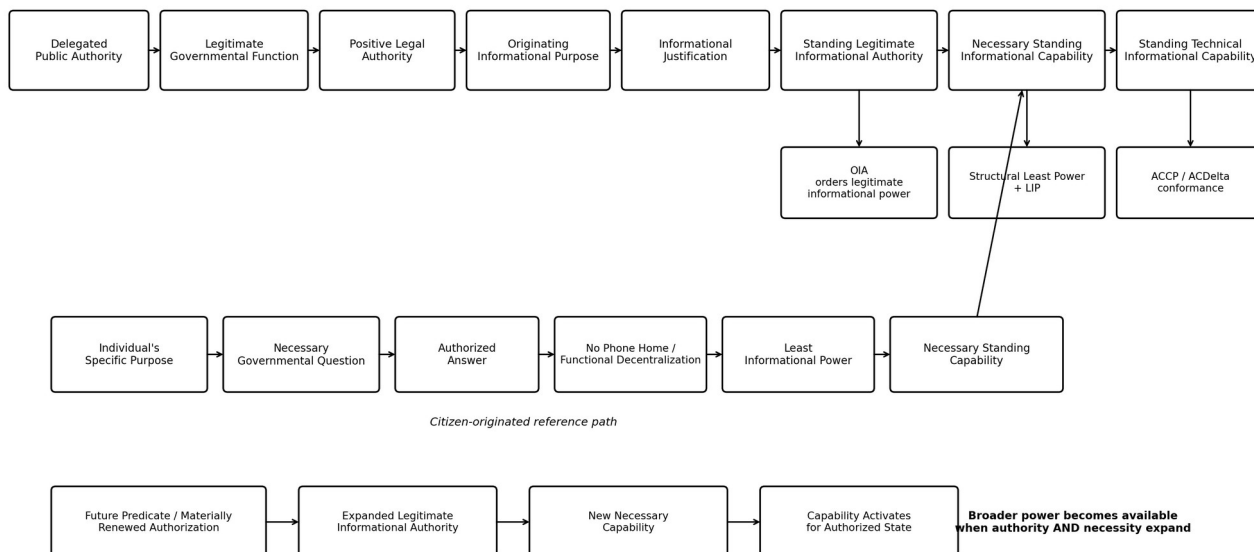


Figure 1. Version 2.2 architecture after IR-01. Legitimate Informational Authority is the outer authority ceiling; Necessary Standing Informational Capability identifies the ordinary standing power actually required; ACCP tests deployed technical capability against that necessity-bounded authority.

PART I. LIMITED GOVERNMENT AND THE POWER TO KNOW

The argument for limited governmental informational power does not require invention of a new constitutional first principle. It begins with a familiar one: public authority is delegated. The difficult question is what that premise means when the power at issue is not taxation, prosecution, licensing, or regulation considered in isolation, but the institutional power to know.

The American constitutional tradition repeatedly describes governmental authority as originating outside the officeholder. Maryland's Declaration of Rights states that government originates from the people and is instituted for the good of the whole. More strikingly, it declares that persons invested with legislative or executive power are "Trustees of the Public" and accountable for their conduct. The point is not that an eighteenth-century state constitution silently incorporated every rule of modern private trust law. It is that public power was understood as entrusted power, held for public purposes and subject to accountability.⁴

The same vocabulary appears in the national founding. Madison wrote of public office as a public trust. Hamilton described impeachment as addressing abuse or violation of public trust. James Iredell, defending the proposed Constitution in North Carolina, emphasized that the people granted representatives particular powers for particular purposes and analogized the instrument to a great power of attorney. Madison's Convention notes add a structural point especially important here. Because those charged with the public happiness might betray the trust, a precaution was to divide the trust among different bodies capable of checking one another.

The historical evidence should not be overstated. Scholars dispute whether the Constitution should literally be classified as a private-law power of attorney, trust, or corporate charter. Modern courts do not generally recognize a freestanding fiduciary cause of action running from every government official to every citizen. Those objections matter. Fiduciary Commons does not depend upon importing private fiduciary doctrine wholesale. Its narrower and more durable premise is that legitimate public authority is delegated, purpose-oriented, accountable, and divided, and that these characteristics support fiduciary obligations concerning how entrusted public power is exercised.⁵

Modern public-fiduciary scholarship develops this proposition more explicitly. Natelson, Lawson, and Seidman have argued in different forms that founding-era public law drew heavily upon fiduciary and agency concepts. Critics such as Primus, Mikhail, Bray and Miller, and Leib and Galoob contest the historical fit, doctrinal transfer, or usefulness of private fiduciary categories in public law. Fiduciary Commons takes that contest seriously. Its claim is not that a label resolves the constitutional analysis. Its claim is that the relationship between the governed and the institutions exercising delegated authority has fiduciary characteristics that become especially important when government acquires durable informational power over persons.⁶

4 Md. Const. Decl. of Rts. arts. 1, 6; Md. Declaration of Rights arts. 1, 4 (1776). Article 6 of the current Declaration describes persons invested with legislative or executive powers as "Trustees of the Public."

5 The Federalist No. 57 (James Madison); The Federalist No. 65 (Alexander Hamilton); 4 Jonathan Elliot, *The Debates in the Several State Conventions on the Adoption of the Federal Constitution* 148-49 (2d ed. 1836) (statement of James Iredell, N.C. Ratifying Convention, July 28, 1788); James Madison, *Notes of Debates*, June 26, 1787, in *The Papers of James Madison*. The historical materials support delegated-power and public-trust propositions; FC's informational consequence is a later synthesis.

6 See Robert G. Natelson, *The Constitution and the Public Trust*, 52 *Buff. L. Rev.* 1077 (2004); Gary Lawson & Guy I. Seidman, *By Any Other Name: Rational Basis Inquiry and the Federal Government's Fiduciary Duty of Care*, 69 *Fla. L. Rev.* 1385 (2017). For substantial critiques, see Samuel L. Bray & Paul B. Miller, *Against Fiduciary Constitutionalism*, 106 *Va. L. Rev.* 1479 (2020); Ethan J. Leib & Stephen R. Galoob, *Fiduciary Political Theory: A Critique*, 125 *Yale L.J.* 1820 (2016); Richard Primus, *The Elephant Problem*, 17 *Geo. J.L. & Pub. Pol'y* 373 (2019); John Mikhail, *Is the Constitution a Power of Attorney or a Corporate Charter?*, 17 *Geo. J.L. & Pub. Pol'y* 407 (2019).

Fiduciary Commons does not answer the public-fiduciary debate by importing the complete private law of trusts into constitutional government. It does not require each public official to maximize the welfare of a discrete beneficiary, does not assume a single governmental maximand, and does not treat every breach of an FC principle as creating a private-law trust remedy. Its narrower claim concerns entrusted public power. Government receives authority for public and legally bounded purposes and exercises informational power under conditions of asymmetry, dependence, and limited citizen exit. In that setting, loyalty, care, confidentiality, non-exploitation, and purpose-bound use are useful and normatively appropriate constraints on delegated informational power. OIA addresses the multiple-person and multiple-purpose problem not by selecting one beneficiary whose interests always prevail, but by ordering which actor may exercise which informational power, for which relationship and purpose, under which authority and consequence. That narrower proposition remains a D3 fiduciary and architectural synthesis where positive law has not independently adopted it.⁷

The next step is conventional administrative law. An agency does not acquire substantive authority because a useful tool becomes available. In *Louisiana Public Service Commission v. FCC*, the Supreme Court stated the principle in direct terms: an agency has no power to act unless Congress confers it, and the agency may not confer power upon itself. The proposition does not mean that every technical implementation requires a new statute. Agencies possess implied and incidental powers necessary to execute lawful grants. It does mean that capability and authority are analytically distinct.

Fiduciary Commons applies that distinction to information systems. Governmental possession of a record is a fact about custody. An application programming interface (API) is a fact about technical accessibility. A data-broker subscription is a fact about commercial availability. An AI model's ability to infer a relationship is a fact about computation. None is, by itself, a source of governmental authority. The legal question must precede the architectural entitlement.⁸

This matters because information is not merely an input to governmental power. In a digital state, the ability to know is itself power. Information determines who becomes visible to government, who is investigated, who qualifies for a benefit, whose license is suspended, which household is flagged, which transaction is considered anomalous, and which prediction becomes an administrative recommendation. The institutional capacity to combine information also changes the range of possible governmental action. A government that can instantly reconstruct relationships across tax, licensing, benefits, location, property, and commercial sources possesses a different practical power from a government whose officers must obtain new authority, approach separate custodians, articulate a purpose, or ask a bounded question before materially expanding what the state knows about a person.

Riley and Carpenter demonstrate why digital capacity matters constitutionally. Riley rejected the idea that a modern cell phone could be treated as an ordinary physical container, emphasizing the qualitative and quantitative difference of digital information. Carpenter recognized that longitudinal location data can provide an intimate chronicle of a person's movements. Chatrue extends the insight. Even a short acquisition can implicate the Fourth Amendment because the underlying Location History system is capable of revealing movements with extraordinary breadth and precision.⁹

7 See Seth Davis, *The False Promise of Fiduciary Government*, 89 *Notre Dame L. Rev.* 1145 (2014); Samuel L. Bray & Paul B. Miller, *Against Fiduciary Constitutionalism*, 106 *Va. L. Rev.* 1479 (2020); Ethan J. Leib & Stephen R. Galoob, *Fiduciary Political Theory: A Critique*, 125 *Yale L.J.* 1820 (2016). FC's narrower response is a D3 synthesis concerning entrusted informational power, not wholesale incorporation of private trust law or its remedial apparatus.

8 *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374-75 (1986). The case establishes the administrative-law proposition that an agency cannot enlarge its own jurisdiction; FC applies that principle by analogy to informational capability.

9 *Riley v. California*, 573 U.S. 373, 393-97, 403 (2014); *Carpenter v. United States*, 585 U.S. 296, 309-13, 320 (2018); Chatrue, 609 U.S. ___, slip op. at 17-29.

Fiduciary Commons therefore distinguishes the lawfulness of an individual informational act from the legitimacy of the standing capability that makes many such acts possible. Existing doctrine often asks whether a particular search, disclosure, match, or use was authorized. That inquiry remains necessary. But a system of delegated power must also ask whether many narrow authorities have been technically recombined into a broader institutional capability that no actor was independently granted.

Federalism illustrates the structural logic. The Constitution distributes authority among sovereigns as well as among branches and institutions. Printz describes the preservation of separate state and federal sovereignty; Bond emphasizes that the diffusion of sovereign power protects individual liberty by denying any one government complete jurisdiction over all concerns of public life. These cases do not establish an information-specific rule against intergovernmental sharing. They do establish the premise that divided authority is not an accidental inconvenience to be engineered away. Fiduciary Commons derives an architectural consequence: interoperability should not silently aggregate the distinct informational authorities of federal, state, and local governments into a generalized collective power to know.¹⁰

The same principle applies within a government. A tax agency's lawful authority is not identical to a health department's authority. A benefits administrator, election official, licensing board, child-protection investigator, and police officer do not possess interchangeable informational mandates merely because all work for the same sovereign. Organizational boundaries are not always constitutional boundaries, and lawful sharing can be extensive. But technical architecture should not assume that common governmental ownership of infrastructure collapses purpose, jurisdiction, or authority.

This produces the first foundational proposition of the paper: informational authority is a species of governmental authority. It should therefore be analyzed according to the same limited-government instincts that govern other public powers. Possession does not create authority. Technical capability does not create authority. Commercial availability does not create authority. Administrative convenience does not create authority. And when government legitimately needs materially broader power, the architecture should be capable of supplying it through a legally sufficient authorization transition rather than by treating generalized access as the default condition of administration.

Throughout this paper, 'government' is often used as institutional shorthand. OIA does not assume that government is a unitary actor. Its analysis disaggregates sovereigns, branches, agencies, programs, officials, contractors, and technical agents according to the authority each can legitimately exercise. The shorthand is useful only so long as the architecture later asks which governmental actor actually holds the relevant authority.

PART II. FROM PRIVACY GOVERNANCE TO INFORMATIONAL POWER

Fiduciary Commons should not be understood as having begun with OIA, ACCP, or the formal Version 1.x architecture. Its earliest identifiable design frame was Utility, Security, and Autonomy. Utility required usable, interoperable, portable, adoptable government services, including guardianship and offline alternatives. Security required verifiability, system protection, and fraud prevention. Autonomy included privacy, confidentiality, control, transparency, recourse, least disclosure, and freedom from government interference or surveillance. The three principles were intended to operate together. This provenance matters because it answers a recurring objection: the framework was not designed to maximize privacy by disabling

¹⁰ Printz v. United States, 521 U.S. 898, 918-25, 935 (1997); Bond v. United States, 564 U.S. 211, 221-23 (2011). These cases establish divided sovereign authority and its liberty rationale; they do not independently establish an information-specific anti-aggregation rule.

government. It was designed to deliver useful and secure digital government without making surveillance capability the hidden price of participation.¹¹

Conventional privacy principles remain an important antecedent. The Privacy Act requires federal agencies to maintain only records relevant and necessary to accomplish a purpose required by statute or executive order, requires disclosure of principal purposes when information is solicited, limits routine uses through compatibility, and regulates computer matching. OECD principles similarly emphasize collection limitation, purpose specification, use limitation, security, openness, individual participation, and accountability. These rules govern information handling powerfully, but Fiduciary Commons extends the inquiry to the architecture that precedes a particular use: what individualized or relational knowledge has government made ordinarily obtainable or constructible, even when every official follows the rules assigned to that system?¹²

The argument so far might appear to restate privacy law in constitutional vocabulary. It does not. Privacy law and information governance already contain many of the principles on which Fiduciary Commons builds. The difference lies in the object being governed.

The federal Privacy Act is a useful example. It requires agencies to maintain only information relevant and necessary to accomplish a purpose required by statute or executive order. It requires agencies soliciting information to identify authority, principal purposes, routine uses, and consequences. A routine use must be compatible with the purpose for which the information was collected. Computer matching is separately regulated through agreements that identify purpose, legal authority, records, and data elements. These are substantial constraints. They show that purpose limitation, necessity, transparency, and bounded correlation are not inventions of Fiduciary Commons.¹³

International and scholarly traditions are equally important. The Organisation for Economic Co-operation and Development (OECD) privacy guidelines articulate Collection Limitation, Purpose Specification, and Use Limitation. Privacy by Design argues that privacy protections should be embedded proactively in systems and organizational practices rather than added after deployment. Nissenbaum's Contextual Integrity offers a sophisticated account of privacy as appropriate information flow according to context, actors, information types, and transmission principles. Information-fiduciary and duty-of-loyalty scholarship identifies relationships in which entrusted information generates duties beyond ordinary notice and consent. Cybersecurity practice contributes least privilege and Zero Trust. Modern digital-identity standards contribute selective disclosure and derived attributes.

Fiduciary Commons is indebted to these antecedents. Its claim is not that existing privacy governance lacks principles. The governance gap lies elsewhere.¹⁴

Most conventional regimes regulate information by asking what may be collected, who may access it, how it may be used, whether it may be disclosed, how long it may be retained, and how it must be secured. These

11 Michael G. Leahy & Timothy Ruff, *Utility, Security, Autonomy (U.S.A.): A Framework of Principles and Goals for Verifiable Government 1-9* (2023-2024 project work, later project copy). Under provenance rule PR-01, the later copy date is not treated as the concept-origin date. See also FC Conceptual Fidelity Audit, Original Thesis Provenance Ledger (Sept. 11, 2026).

12 5 U.S.C. § 552a(a)(7), (b)(3), (e)(1), (e)(3), (o); Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896, 1896 (1974); OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* paras. 7, 9-10 (as amended 2013). These are strong privacy and purpose-limitation antecedents, not sources of ACCP or OIA.

13 5 U.S.C. § 552a(a)(7), (b)(3), (e)(1), (e)(3), (o); Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896, 1896 (1974).

14 OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* paras. 7, 9-10 (as amended 2013); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004); Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information & Privacy Commissioner of Ontario 2011); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 Wash. U. L. Rev. 961 (2022).

are indispensable transactional and lifecycle questions. But the architecture of modern government can create an institutional capability that is broader than any single transaction. Once a shared identity layer, cross-domain query service, analytics platform, broker subscription, or AI agent is available across programs, the government's practical ability to know may be materially broader than the permissions exercised in the ordinary case.

Security controls do not necessarily solve that problem. A perfectly secured generalized capability remains generalized capability. Encryption can protect a data lake against outsiders while leaving the government with universal internal query power. Zero Trust can require strong authentication and per-request authorization while the authorization policy itself permits cross-purpose search. Audit can reveal that every official acted within assigned permissions even when the permission architecture grants the institution excessive standing power. The question is not only whether the system is secure against unauthorized use. It is whether the authorized capability is itself appropriately bounded.

Nor does data minimization necessarily answer the problem. Consider an age-verification transaction. National Institute of Standards and Technology (NIST) federation guidance recognizes that a relying party may need only a derived Boolean answer indicating that a person meets an age threshold, rather than the person's full birth date. That is sound minimization. But imagine that the verification service logs every presentation, resolves each relying party, retains time and location metadata, and makes those logs available to government analysts. The attribute disclosed to the verifier has been minimized while the institutional surveillance capability has expanded.

This is why No Phone Home is more than a technical privacy preference. A verification architecture can reveal little to the immediate verifier while allowing an issuer, identity provider, or central service to observe who presented which credential, to whom, when, and in what context. U.S. Department of Homeland Security (DHS) decentralized-identity requirements have recognized this problem technically by seeking to eliminate phone-home behavior and hidden issuer-verifier back channels. Fiduciary Commons supplies an authority-based reason: the authority to attest that a credential is valid does not automatically include authority to observe every downstream use of that credential.¹⁵

The same distinction appears in least privilege. NIST defines least privilege by limiting resources and authorizations to what is necessary to perform assigned functions. Zero Trust Architecture emphasizes accurate, least-privilege, per-request access decisions and rejects implicit trust based merely on network location. Those principles are important architectural antecedents. ACCP asks a different question. Least privilege ordinarily asks what permissions an actor or process needs inside a system. ACCP asks what informational capability the governmental system itself should possess before additional public authority exists.

That distinction becomes visible when everyone complies. Suppose a state has carefully defined roles. Each employee sees only what the employee's role permits. Administrators are logged. Queries are authenticated. Yet a small set of authorized roles can search every program, a shared AI service can correlate across domains, and a vendor platform can enrich results with commercial data. No unauthorized access occurs. Traditional access governance may report success. The limited-government question remains: why does the institution possess that standing capability?¹⁶

15 Nat'l Inst. of Standards & Tech., Digital Identity Guidelines: Federation and Assertions, NIST SP 800-63C-4 §§ 3.11.2, 7.3 & examples (2025) (describing derived attribute values, including Boolean age assertions).

16 Nat'l Inst. of Standards & Tech., Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, AC-6; Scott Rose et al., Zero Trust Architecture, NIST SP 800-207, at 4-7 (2020). These are security-authorization antecedents, not sources of governmental informational authority.

Privacy by Design comes closer because it insists that privacy be embedded into architecture. Rosenzweig's 2003 testimony concerning government surveillance systems comes closer still. He argued that technology should implement existing legal limitations and should not itself become a basis for new governmental powers or capabilities. Fiduciary Commons should claim no priority over that intuition. Its contribution is to formalize the relationship at the level of governmental informational power: standing technical capability should approximate standing legitimate informational authority, and materially greater capability should become available through a legitimate authorization transition.

The shift is subtle but consequential. The object of minimization becomes governmental informational power, not simply data volume. The object of decentralization becomes effective power, not physical storage. The object of authorization becomes not merely user access but the government's institutional ability to obtain, verify, correlate, infer, retain, disclose, and act. And the central compliance question becomes structural: what can government know without obtaining materially new authority?¹⁷

This is the governance gap that OIA is designed to fill. Privacy remains essential because persons have legitimate interests in secrecy, context, dignity, autonomy, and freedom from surveillance. Security remains essential because entrusted information must be protected from compromise. Transparency and accountability remain essential because public institutions must be reviewable. But none of those objectives alone determines the proper distribution of governmental power to know.

A system can be private in one sense and overpowered in another. It can disclose little publicly while enabling comprehensive internal government correlation. It can be secure while institutionally overbroad. It can be transparent about a capability that government should not possess. It can obtain formal consent in circumstances where the person has no meaningful alternative. The inquiry therefore has to move from information practices to informational authority.

PART III. GENERALIZED INFORMATIONAL POWER

Generalized Informational Power is the condition in which many bounded authorities to know become a reusable, cross-purpose governmental capacity to construct materially broader individualized knowledge. The concept is functional. It does not depend upon a single database, a single identifier, or a single agency.

This point is necessary because the familiar image of informational centralization is a data lake: many agencies send records into one repository, identities are resolved, and authorized users search the combined environment. That architecture plainly creates concentration risk. But modern systems can reproduce much of the same effective power while leaving every source database physically separate. A federated query layer can search them in real time. A common identity service can resolve the same person across domains. APIs can make records machine-accessible. A commercial intermediary can enrich government queries. An AI agent can call multiple services and synthesize the result. Metadata can reveal relationships that the underlying content does not. The architecture can therefore be distributed in topology and centralized in power.

This is the controlling meaning of functional decentralization: decentralization must be evaluated by effective informational power rather than by network diagram. Physical separation can be valuable for resilience, cybersecurity, organizational autonomy, and privacy. But it is not sufficient if government retains standing centralized query, correlation, inference, observation, or retrieval capability.

¹⁷ Paul Rosenzweig, *Securing Freedom and the Nation: Collecting Intelligence Under the Law*, testimony before the H. Permanent Select Comm. on Intelligence (Apr. 9, 2003) (arguing that technology should implement existing legal limits and should not itself become the basis for new governmental powers or capabilities).

The converse is also important. A centralized component is not automatically illegitimate. A narrowly bounded licensing database, maintained for a defined population and purpose, may be entirely consistent with limited informational authority. The relevant question is not whether a server is centralized. It is whether many limited grants of authority have been transformed into generalized standing power.

Chatrre illustrates why capability matters. The Court did not conclude that two hours of movement are inherently so revealing that any acquisition must be a search. Its reasoning attends to the character of Location History as a system capable of reconstructing movements with breadth and precision. The majority's concern with the surveillance instrument helps explain why later selection of a narrow interval does not erase the scope of the invasion. Justice Jackson's concurrence pushes the problem toward authorization architecture. She objected that later stages of the geofence process could expand the information available to officers without renewed magisterial justification and criticized the resulting discretion as a roving commission.

The lesson should again be stated carefully. Chatrre regulates a search. It does not establish a constitutional rule for every standing information system. But it demonstrates that digital capability can matter to constitutional analysis even when the government ultimately reviews a narrow slice of information. Fiduciary Commons generalizes that insight beyond the geofence context.¹⁸

Contemporary scholarship is beginning to ask a similar structural question. D.E. Wright's 2026 Fusion Architecture argues that distributed surveillance components can collectively produce a standing governmental capability that no single component possesses and no institution independently authorized. That work is close enough to foreclose any responsible claim that Fiduciary Commons alone discovered standing governmental capability as a constitutional object. The difference is scope and architecture. Fiduciary Commons treats standing capability as a general problem of delegated informational authority across administration, benefits, identity, regulation, fraud, AI, procurement, and surveillance. It also distinguishes standing capability from capability that becomes available only after an authorization state changes.¹⁹

That distinction answers one of the strongest objections to purpose sequestration. Modern government is relational. Benefits depend on income. Licensing may depend on criminal or professional records. Fraud may span programs. Public health crosses institutional boundaries. Emergencies require coordination. If every legitimate interaction eventually requires interoperability, perhaps purpose-specific architecture simply relocates integration from storage into the query layer and recreates the same generalized power.

The objection is serious. The answer is not to deny that government may sometimes need the same information that a fully integrated system could provide. The answer is to distinguish eventual lawful capability from standing capability. A government may be entitled, after a fraud predicate matures or a court issues process or a statute authorizes a match, to correlate information that it could not ordinarily correlate. The architecture can make that operation possible. But the broader capability need not exist as an ordinary, reusable entitlement before the authority transition occurs.

Federal fraud law provides a useful test because it prevents the theory from becoming privacy absolutism. Congress has expressly authorized significant data matching and analytics in particular program-integrity contexts. The Do Not Pay Initiative authorizes review of designated databases for eligibility and improper-payment purposes. Medicare and Medicaid law authorizes an integrated data repository and interagency

18 Chatrre, 609 U.S. ___, slip op. at 21, 29-32; id. at 1-4 (Jackson, J., concurring). The majority makes the capability of the surveillance instrument salient but does not hold that standing surveillance architecture is independently unconstitutional.

19 D.E. Wright, Fusion Architecture: Standing Governmental Capability and the Fourth Amendment: A Constitutional Framework for Distributed Domestic Surveillance (Jan. 8, 2026), SSRN (posted Aug. 1, 2026). Wright independently proposes standing distributed governmental capability as a Fourth Amendment object. FC therefore does not claim priority for the general standing-capability insight.

matching for fraud, waste, and abuse. Congress has also required predictive analytics using large datasets, provider networks, billing patterns, and beneficiary-utilization patterns.

Those statutes are not embarrassing exceptions to Fiduciary Commons. They demonstrate the theory's central premise. Broader informational capability can be legitimate when broader authority has actually been granted. The question becomes whether the implemented capability corresponds to that authority: which programs and populations are included, which sources may be used, which operations are permitted, which inferences may be drawn, which consequences may follow, who may exercise the capability, and whether the capability remains available for unrelated purposes after the authorized function ends.²⁰

Generalized Informational Power can therefore arise through several pathways. One is aggregation: many records become a comprehensive profile. A second is correlation: records remain separate but can be joined through common identifiers or resolution services. A third is inference: machine analysis derives materially new individualized knowledge from lawful source data. A fourth is observability: a central actor learns about transactions merely because verification or routing passes through it. A fifth is reacquisition: government obtains through a commercial intermediary information that it could not ordinarily construct from its own purpose-bounded systems. A sixth is delegation: a broadly capable service becomes available across agencies, converting specialized powers into shared infrastructure.

None of these pathways is necessarily unlawful. Each is authority-bearing when it materially expands what government can know or do. That is the point.

The historical general-warrant analogy illuminates the risk without resolving the doctrine. The Fourth Amendment's particularity requirement developed against forms of search authority characterized by breadth and official discretion. Stanford described the general warrant as the kind of authority the Amendment was designed to forbid. Berger treated electronic surveillance with particular suspicion when authorization was broad and insufficiently particular. Garrison emphasized that particularity prevents wide-ranging exploratory searches. Steagald and Ybarra reinforce the principle that authority concerning one object or person does not automatically become authority concerning another.

FCGIAS therefore uses a General-Warrant Diagnostic rather than claiming an established judicial "Otis Test." The relevant characteristics are breadth, standing or indefinite availability, discretionary exercise, lack of particularity, delegation, and generalized applicability. The diagnostic asks whether modern architecture functionally recreates those characteristics. The stronger proposition, that a database architecture itself completes a Fourth Amendment violation merely by creating surveillance capability, remains a proposed constitutional development rather than current Supreme Court doctrine.²¹

Generalized Informational Power also explains why purpose matters structurally. A broad label such as public safety, fraud prevention, service improvement, analytics, or efficiency cannot by itself determine informational scope. These are legitimate governmental objectives, but if they function as permanent predicates for cross-domain access, they cease to constrain. Purpose Particularity asks whether an independent reviewer can identify the governmental function, the relationship or authority supporting it, the information reasonably necessary, the permitted operations, the endpoint, and what additional authority would be required to expand it.

Question Particularity narrows the problem further. In population-scale or analytical activity, what question

20 31 U.S.C. § 3354(a)-(d); 42 U.S.C. §§ 1320a-7k(a), 1320a-7m(a)-(c). These provisions affirmatively authorize significant matching, integrated data, and predictive analytics for specified program-integrity purposes.

21 *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Stanford v. Texas*, 379 U.S. 476, 481-86 (1965); *Marron v. United States*, 275 U.S. 192, 196 (1927); *Berger v. New York*, 388 U.S. 41, 54-60 (1967); *Steagald v. United States*, 451 U.S. 204, 212-22 (1981); *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

is government authorized to ask? A fraud unit may be authorized to test a defined predicate against specified sources. That does not necessarily imply authority to explore every relationship revealed along the way. A benefits program may be authorized to determine household eligibility. That does not necessarily imply authority to ingest the household's entire financial history. A licensing agency may be entitled to know whether a disqualifying condition exists without acquiring the complete record from which the answer is derived.

This leads to a central distinction that the remainder of the paper will develop: government often needs an Authorized Answer rather than an informational environment. The distinction is already technically familiar. NIST recognizes derived attributes that allow a relying party to receive a Boolean age determination instead of a birth date. Digital credentials can disclose selected attributes. Distributed systems can execute bounded queries. These techniques are not inventions of Fiduciary Commons. The framework changes the reason for preferring them. The objective is not only to disclose less data. It is to avoid creating unnecessary governmental power to know.

Generalized Informational Power is therefore the problem to which OIA responds. OIA does not require information to remain isolated. It requires power to remain ordered. It permits interoperability but rejects silent authority aggregation. It permits correlation and inference but treats material expansion as something that must be justified. It permits government to become more capable when lawful authority expands, but resists constructing the maximum possible capability in advance and relying on policy to promise restraint.

The next question is why the person, rather than the institution possessing the largest database, should occupy the primary normative position in that ordering. That is the work of Fiduciary Commons.²²

D. The General-Warrant Diagnostic and the Limits of Current Doctrine

The General-Warrant Diagnostic should be understood at three levels. The first is historical. The founding objection to general warrants and writs of assistance concerned broad authority, weak particularization, official discretion, and the ability to search without a sufficiently bounded object. That history supplies a structural suspicion of generalized governmental power, but it does not mechanically answer modern questions about databases, APIs, or AI.²³

The second level is current doctrine. Particularity doctrine constrains warrants and searches; Riley, Carpenter, and Chatrre recognize that digital systems can alter the constitutional significance of information by changing its comprehensiveness, persistence, and accessibility. Chatrre is especially important because the majority evaluated the government's acquisition in light of the Location History system's capacity to reveal movements, while Justice Jackson focused on the risk that a staged process could expand without renewed judicial control. Current doctrine therefore makes digital capability and authorization scope relevant to adjudicating particular governmental acquisitions.

The third level is the Fiduciary Commons (FC) proposal. Fiduciary Commons argues that certain standing informational capabilities should themselves become objects of public-law scrutiny when they functionally create the characteristics that the general-warrant tradition distrusted: broad reusable access, weakly particularized purpose, discretionary cross-purpose inquiry, and authority that becomes effectively general through architecture. That proposition is not the holding of Chatrre, Carpenter, or any other Supreme Court

²² NIST SP 800-63C-4 §§ 3.11.2, 7.3 & examples (2025); FCGIAS Version 2.2, Consolidated Controlling Edition § 20 (Authorized Answer Principle). The technical mechanism is an antecedent; FC supplies the public-authority rationale.

²³ FCGIAS Version 2.2, Consolidated Controlling Edition, Part XXV, § 98, and § 133. The Standard deliberately separates its General-Warrant Diagnostic and proposed D4 architectural constitutional argument from controlling Fourth Amendment doctrine.

case cited here. It is a proposed development derived from the interaction of limited-government structure, digital-search doctrine, fiduciary obligation, and modern system capability.

The capability-centered claim must also be stated with appropriate originality discipline. D.E. Wright's 2026 work on fusion architecture independently argues that distributed integration of otherwise lawful systems can create a standing governmental surveillance capability that no component possesses alone. Fiduciary Commons therefore does not claim priority for the general insight that distributed standing capability can itself be constitutionally significant. Its narrower claimed contribution lies in joining that problem to OIA, fiduciary informational relationships, Originating Informational Purpose, Authorized Answer, Least Informational Power, authorization transitions, procurement, statutory translation, and formal conformance.²⁴

Chatrie is therefore most valuable to FC when used neither timidly nor extravagantly. It does not prove the architectural thesis. It demonstrates that constitutional analysis cannot always be confined to the small slice of data ultimately viewed by an officer while ignoring the character of the instrument through which government acquired it. FC takes that insight from the adjudicated search to the design of governmental systems and asks a prior institutional question: should ordinary standing architecture place the broader instrument in government's hands before a sufficiently particular authority state exists?²⁵

PART IV. FIDUCIARY COMMONS

The problem of governmental informational power cannot be solved by architecture alone because architecture has to be ordered toward a theory of legitimate relationship. Fiduciary Commons supplies that theory. Its starting point is a rejection of a familiar but misleading premise: facts concerning persons are not best understood as objects of ownership simply because an institution records, stores, or processes them.

This proposition requires precision. Law can protect records, compilations, databases, trade secrets, copyrighted selection or arrangement, and other informational artifacts. Feist distinguishes facts from copyrightable compilations; Ruckelshaus demonstrates that some informational interests, such as trade secrets, can constitute property for particular legal purposes. Fiduciary Commons does not deny those doctrines. It distinguishes the underlying factual reality concerning a person from the artifact through which that reality is memorialized, organized, or commercially protected. The institution that records a fact may own a server, a database product, or intellectual property in a compilation. That does not establish exclusive normative dominion over the fact concerning the person.²⁶

The distinction matters because an ownership model asks the wrong first question. If information is treated primarily as property, governance tends to revolve around possession, transfer, license, consent, and exclusion. Those concepts can be useful, but they fit poorly where the same fact is simultaneously relevant to the person, a government program, a physician, an employer, a court, or another participant in a legitimate relationship. A fact may be true without being exclusively ownable. The more useful question is therefore not “Who owns the fact?” but “Who has legitimate authority to know, use, disclose, verify, or act upon it, for what purpose, and subject to what duties?”

24 D.E. Wright, *Fusion Architecture: Standing Governmental Capability and the Fourth Amendment: A Constitutional Framework for Distributed Domestic Surveillance* (Jan. 8, 2026), SSRN (posted Aug. 1, 2026). Wright independently develops the standing distributed-capability problem. FC's claimed contribution is narrower and rests in the combined fiduciary, authority, purpose, least-power, procurement, statutory, and conformance architecture.

25 Chatrie, 609 U.S. ___, slip op. at 21, 29-32; id. at 1-4 (Jackson, J., concurring); Michael G. Leahy, *The Architecture the Court Cannot Build: Chatrie v. United States and the Case for Fiduciary Governance of Government Data* (July 23, 2026) (unpublished manuscript). The architectural conclusion in the text is FC's extension, not Chatrie's holding.

26 Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344-51 (1991); Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1001-04 (1984); Ignacio Cofone, *Beyond Data Ownership*, 43 Cardozo L. Rev. 501 (2021). These authorities support the fact/artifact and property-model qualifications; they do not establish FC's complete commons theory.

Fiduciary Commons calls the domain of such factual information a commons not because everyone is entitled to access it, but because the underlying factual reality is not appropriately reduced to exclusive dominion. The commons is governed through authority and entrustment. The concept therefore differs from both public-domain rhetoric and data-ownership rhetoric. Unownable does not mean unprotected. It means that protection should be grounded in legitimate relationships, duties, authority, and purpose rather than in a fiction that every fact must have an owner.

The individual occupies the primary normative position in this structure. Fiduciary Commons describes the person as the Primary Information Trustee, or PIT, with respect to information concerning that person. Again, “trustee” is not a claim that the person holds conventional property title to every fact. It identifies the person as the presumptive locus of informational authority where no superior lawful authority exists. The person ordinarily decides whether to disclose a credential, authorize a private transaction, present proof, or delegate authority to another. Government does not become primary merely because it operates the largest information system.

This principle has roots in the pre-formal development of the framework. The earlier Utility, Security, Autonomy work placed individual control, delegation, guardianship, least disclosure, specific purpose, confidentiality, recourse, offline alternatives, and decentralization inside the design problem before Fiduciary Commons had been formally articulated. The later PIT concept did not invent those concerns. It supplied a jurisprudential account of why they belong together.²⁷²⁸

Some persons cannot exercise informational authority personally in every context. Children, persons under disability, and others acting through lawful representatives require a structure for delegated or substituted authority. Fiduciary Commons therefore recognizes the Authorized Information Trustee, or AIT. An AIT does not become a universal substitute owner of another person's information. The authority is bounded by the legal relationship that creates it, such as parenthood, guardianship, agency, or another recognized delegation, and should be technically representable so that systems can distinguish the principal, the representative, the scope of authority, and its duration.

This is more than an identity-management feature. A system that cannot represent bounded human delegation often solves the problem by creating shared credentials, administrative overrides, or institutional master access. Those workarounds convert a legitimate relationship into generalized technical authority. AIT is therefore an example of the larger FC method: represent the real authority relationship rather than compensating for its absence with broader system power.

Government occupies a different position. When government legitimately obtains information concerning a person, it does not thereby become the primary informational authority. It becomes a secondary informational fiduciary within the governmental relationship that justified the acquisition. The term “secondary” does not mean unimportant or subordinate to individual preference in every case. Government can possess coercive authority that overrides individual objection. It can compel tax information, investigate crime, adjudicate disputes, regulate licensed activity, protect children, administer benefits, and respond to emergencies. The point is that its informational authority is derivative of legitimate public authority and remains bounded by the purpose, jurisdiction, and legal relationship that justify it.

27 Michael G. Leahy & Timothy Ruff, *Utility, Security, Autonomy (U.S.A.): A Framework of Principles and Goals for Verifiable Government 1-9* (2023-2024 project work, later project copy) [hereinafter USA V1]. Under project provenance rule PR-01, the later copy date is not treated as the concept-origin date.

28 PERSONAL DATA TRUSTEESHIP ACT, Version 2.2 TRI-PATCH-01, §§ 2-4 (Sept. 13, 2026) (Model Act Freeze Candidate) [hereinafter PDTA 2.2]. The draft defines PIT without relying on ownership and expressly preserves lawful governmental authority and the rights of other persons.

This is where the founding-era fiduciary premise becomes operational. If governmental power is delegated and held for public purposes, informational power acquired in the exercise of that authority should carry corresponding duties. Fiduciary Commons emphasizes loyalty to the legitimate public purpose, care in the exercise of informational power, confidentiality where appropriate, minimization, purpose fidelity, and resistance to self-expansion. The government should not exploit informational asymmetry merely because custody or technology makes exploitation possible.²⁹

Consent does not solve the governmental problem. In private relationships, meaningful consent can create legitimate authority for many informational acts. Government often acts under a different source of authority. A taxpayer cannot withdraw consent from lawful tax administration. A criminal suspect need not authorize a valid search warrant. A benefits applicant may have choices about applying, but once a program is invoked the agency's authority and duties arise from law, not from a click-through privacy notice. Fiduciary Commons therefore refuses to treat consent as a universal solvent. Consent may authorize what the individual is entitled to authorize. It cannot manufacture governmental power that the individual does not possess or erase legal limits imposed for public reasons.

Purpose performs the limiting work that ownership and consent cannot. Governmental information is acquired within a relationship and for a function. Purpose sequestration seeks to preserve that relationship architecturally. Records may be held by government, but their availability for one lawful function does not automatically make them standing resources for every other function. A purpose domain is therefore not merely a folder or access-control group. It is an informational boundary derived from legitimate authority.

Purpose sequestration does not prohibit sharing. It requires sharing to be justified. A new purpose may rest on the same statute, a compatible-use rule, another statute, judicial process, an emergency authority, an individual request, or some other legally sufficient basis. The relevant question is whether the second use is genuinely within existing authority or constitutes a material expansion. The architecture should make that distinction visible rather than allowing the mere existence of a record to answer it.

This explains the phrase “Fiduciary Commons.” The commons describes the nonexclusive character of factual reality. Fiduciary describes the duties and authority relationships through which access to that reality is legitimately ordered. The combination avoids two symmetrical errors. One is institutional dominion: because government collected the information, government may treat it as a general governmental asset. The other is absolute individual ownership: because the information concerns the person, no legitimate public authority may use it without personal permission. Fiduciary Commons rejects both.

The result is a theory of ordered relationships. The person is primary where personal authority governs. Authorized representatives exercise bounded delegated authority. Government acts as a secondary informational fiduciary when legitimate public authority justifies informational action. Different agencies, programs, institutions, and sovereigns hold different authority. Vendors remain private actors governed by law and contract rather than becoming governmental fiduciaries merely by providing technology. The architecture must preserve these distinctions.

The framework's normative ambition is therefore broader than privacy. Privacy asks, among other things, when information about a person should remain inaccessible or flow only under appropriate conditions. Fiduciary Commons asks how legitimate informational authority should be allocated among the actors who stand in different relationships to the same factual reality. Once the question is framed that way, the problem of generalized governmental capability becomes a problem of authority ordering.

That is the transition to OIA.

²⁹ See Md. Const. Decl. of Rts. art. 6; Natelson, *supra* note 5; Lawson & Seidman, *supra* note 5; Balkin, *supra* note 10; Richards & Hartzog, *supra* note 10. FC's proposition that informational authority is a species of delegated public authority is a structural and normative synthesis, not a settled freestanding cause of action.

A. Why Informational Power Carries Fiduciary Constraints

The fiduciary claim can now be stated without relying on metaphor. Public authority is delegated power to alter legal relations, distribute benefits and burdens, compel conduct, investigate, adjudicate, and otherwise act in the name of the polity. Information is one of the principal means through which those powers are exercised. Government identifies the person to whom a rule applies, determines facts relevant to a benefit or sanction, verifies predicates, forms judgments, and creates records that can affect later governmental action. Informational authority is therefore not merely custody ancillary to public power. It is a mode of exercising public power. If the legitimacy of the underlying power depends upon delegation, purpose, accountability, and limits, the informational acts through which that power is exercised inherit those characteristics. This is the bridge from fiduciary government to informational fiduciary duty.

The PIT proposition likewise requires more than rejection of ownership. The person's primary position rests on the convergence of four considerations. First, information concerning a person can affect that person's liberty, opportunities, reputation, relationships, and ability to participate in civic and economic life. Second, the person ordinarily possesses authority to decide whether to reveal facts about self in voluntary relationships, subject to the legitimate rights of others. Third, governmental authority is derivative: government must identify a lawful public basis for compelling, obtaining, or using information where personal authorization is absent. Fourth, institutional custody is contingent. A record may move among institutions while the person to whom the information relates remains the continuous human subject of the consequences. PIT therefore identifies a presumptive locus of authority, not a proprietary title.

The presumption is not absolute. A person cannot use PIT to veto a valid subpoena, conceal taxable income from lawful administration, prevent a court from maintaining an adjudicatory record, or erase another person's legitimate informational interests. PIT instead establishes the baseline from which contrary authority must be justified. Where government acts coercively, the source of authority is law rather than personal permission. Where another person possesses an independent right or interest, the information cannot be reduced to unilateral control by either person.

Relational information demonstrates why this matters. A marriage record concerns two persons. A parent-child relationship concerns each member of the family. A communication concerns sender and recipient. A joint account, property interest, professional relationship, allegation, or transaction may be information about several persons at once. No coherent ownership rule can make each person exclusive owner of the same factual relationship. Fiduciary Commons instead asks what authority each participant and institution possesses with respect to the relationship, what duties accompany that authority, and which uses require additional justification. Relational information therefore strengthens, rather than weakens, the commons thesis: factual reality can be shared in relevance without being universally accessible.³⁰

This relational account also disciplines governmental design. A government system should not assume that authority derived from one person's transaction supplies unlimited authority over every other person revealed by the same record. A benefits investigation may legitimately reveal a household member; a fraud analysis may reveal a network; a licensing inquiry may reveal an employer or complainant. The emergence of the relationship can be necessary to the authorized function. Further use of the newly visible person or relationship may nevertheless require a distinct authority analysis. The architecture should preserve that distinction where the expansion is material.

PART V. ORDERED INFORMATIONAL AUTHORITY

Ordered Informational Authority is the general theory of legitimate informational power developed through Fiduciary Commons. It concerns the allocation of power to obtain, verify, know, correlate, infer, disclose,

³⁰ PDTA 2.2 § 3 (defining Relational Information); FCGIAS Version 2.2, Consolidated Controlling Edition control CF-34. Relational information is one reason FC rejects exclusive personal ownership as the governing model.

retain, and act upon information according to legitimate relationships, purposes, jurisdiction, and authority. Its central proposition is simple: government should not construct generalized informational power.

The proposition is not a ban on government knowledge. It is a rule about how governmental power to know becomes legitimate. A licensing agency may know what its lawful function requires. A court may compel information under judicial authority. A fraud investigator may acquire broader information when a lawful predicate and governing authority permit it. A public-health agency may act under emergency or statutory powers. OIA does not require every informational act to originate with the individual. It requires the informational power exercised to have a legitimate source and to remain ordered to that source.³¹

The word “ordered” does substantial work. Information systems tend toward reuse. Once a record has been collected, the marginal technical cost of using it again is low. Once an API exists, additional consumers can be added. Once identities are resolved, correlation becomes easier. Once an AI service can call several systems, adding another source may require only a configuration change. Technical systems therefore create pressure toward capability accumulation.

Law does not necessarily move the same way. Authority is distributed by function, office, program, proceeding, jurisdiction, sovereign, and purpose. It may be temporary. It may depend on predicates. It may be reviewable by a court or another official. It may expire. It may authorize an answer without authorizing permanent acquisition of the source material. OIA is the discipline of making technical capability respect those differentiated legal states rather than silently flattening them.

This distinguishes OIA from Contextual Integrity while acknowledging a significant intellectual antecedent. Contextual Integrity asks whether information flows are appropriate to a social context according to actors, attributes, and transmission principles. OIA likewise rejects the idea that information can be governed without regard to relationship and purpose. But OIA's organizing object is governmental power. It asks not only whether a flow is contextually appropriate, but what institutional capability government is entitled to possess, which actor may exercise it, under what authority, and what must happen before that capability can materially expand.

The distinction also separates OIA from ordinary access control. An access-control system begins with resources and permissions. OIA begins with authority. The question is not first which role should receive a permission, but whether government should possess the underlying capability at all, whether the role's institution is the proper holder of it, and whether the capability should exist before a triggering authorization event.³²

The master OIA test can therefore be stated as follows: What is the most extensive individualized knowledge government can obtain using the standing legal and technical authority built into this architecture, and what additional authority must government obtain before it can know materially more?

This test deliberately assumes compliance. It is designed to expose a class of failures that conventional security analysis can miss. If a system is dangerous only when an administrator steals credentials, the problem may be security. If the system allows a properly authorized administrator, analyst, agent, or service to construct a cross-purpose population profile under ordinary permissions, the problem is architectural authority.

31 FCGIAS Version 2.2, Consolidated Controlling Edition, Parts II-IV; PDTA 2.2 § 3. OIA is an FC synthesis and organizing theory, not a claim of existing positive law.

32 Nissenbaum, *supra* note 10; 5 U.S.C. § 552a; OECD Privacy Guidelines, *supra* note 10. These are important relational and purpose-limitation antecedents. OIA differs by making legitimate governmental informational power and standing capability its organizing objects.

The distinction between standing and authority-contingent capability is central. Standing capability is informational power available under the ordinary legal and technical state of the system. Authority-contingent capability is power that can become available after a legally sufficient authorization transition. The latter is not fictitious merely because it is unavailable in the ordinary state. A court order can activate access. An emergency declaration can alter permissions. A statutory fraud predicate can permit a defined match. An individual's request can authorize a service transaction. A supervisor or independent official can approve an operation where law makes that approval sufficient.

A system need not keep every possible power permanently enabled in order to remain useful. It can be designed to change state.

Materially Renewed Authorization names the transition. “Renewed” does not mean that every informational expansion requires a warrant, a new statute, or even a new human decision. The legally sufficient event depends on the governing regime. It may be consent, delegated authority, an administrative predicate, statutory authorization, judicial process, emergency authority, or another lawful basis. What matters is that a material expansion in purpose, scope, persons or objects, domains, correlation, inference, use, duration, or consequence is not treated as a silent inheritance from a narrower authorization.

This principle answers the practical objection that architecture cannot anticipate every legitimate future need. It need not. It must represent the boundary between what is presently authorized and what becomes authorized after an appropriate transition.³³

Correlation and inference are especially important because they reveal why possession-based governance is incomplete. Government may lawfully possess two records and still create materially new knowledge by joining them. It may lawfully possess a dataset and derive a prediction that materially changes how a person is classified or treated. The operation, not merely the source data, can therefore be authority-bearing.

Fiduciary Commons does not claim that every computational inference requires new legal process. Ordinary arithmetic, validation, deduplication, or analysis within a lawful purpose can remain inside existing authority. The trigger is materiality. Does the operation produce materially broader individualized knowledge, expose a new relationship, cross a purpose or jurisdictional boundary, or enable a materially different governmental consequence? If so, OIA requires the authority for that expansion to be identified.³⁴

OIA also has a federalism dimension. Governmental informational authority is distributed among sovereigns as well as agencies and programs. A state may lawfully possess information for a state function; the federal government may possess different authority; a locality may possess still another. Intergovernmental cooperation can be legitimate and necessary. But interoperability does not itself aggregate the legal authorities of the participating governments.

The rule is Jurisdictional Non-Aggregation: technical connection among governments should not create a standing collective informational power greater than the authority that can legitimately be exercised in the particular transaction. Where law authorizes joint operations or sharing, the architecture may reflect that authority. Where it does not, the fact that systems can communicate is not a substitute.³⁵

33 FCGIAS Version 2.2, Consolidated Controlling Edition § 28; PDTA 2.2 §§ 3, 8-10. 'Materially Renewed Authorization' denotes a distinct, reviewable authorization event sufficient under the applicable legal regime; it does not prescribe a warrant or statute in every context.

34 PDTA 2.2 §§ 8-10. The Act separately governs informational operations and defines Material Secondary Correlation, Materially Renewed Authorization, Question Particularity, and Purpose Sequestration.

35 Printz, 521 U.S. at 918-25, 935; Bond, 564 U.S. at 221-23; FCGIAS Version 2.2, Consolidated Controlling Edition (distributed governmental authority and intergovernmental controls). The anti-aggregation rule is FC's architectural consequence, not an information-specific holding of Printz or Bond.

OIA therefore offers a different account of interoperability. Conventional digital-government strategy often treats interoperability as an unqualified good because it reduces friction and improves service. OIA treats interoperability as a capability that must be designed according to authority. The goal is not maximum connection. It is legitimate connection.

A conforming system may be highly interoperable at the transaction layer while refusing standing cross-purpose access. It may answer a specific eligibility question without transferring a source record. It may permit a fraud unit to execute an authorized match without giving the unit general browsing access to participating databases. It may allow a credential to be verified without informing the issuer where the credential was presented. It may allow an AI agent to call a service only when the governmental function represented by the agent is authorized to make that call.

The result is a theory of informational limited government. Limited government does not mean that government is always weak. It means that governmental power is justified, bounded, and reviewable. OIA applies that structure to knowledge. Government should be able to know what it is legitimately authorized to know. It should be structurally constrained from knowing materially more through ordinary standing access. It should become capable of knowing more when legitimate authority itself has materially expanded.

The next architectural consequence follows from the fact that legitimate informational authority is already distributed. If authority is distributed, architecture should not unnecessarily centralize the power that exercises it.

PART VI. DECENTRALIZED INFORMATIONAL AUTHORITY

Decentralization is a core principle of Fiduciary Commons because informational authority is distributed before a system is designed. Persons possess personal informational authority. Parents and guardians may exercise bounded delegated authority. Programs possess statutory responsibilities. Agencies possess distinct missions. Courts exercise judicial authority. States, localities, and the federal government occupy different jurisdictions. Private institutions possess their own lawful interests and duties. The architecture should begin from that distribution rather than assume that efficiency requires its collapse.

This is Decentralized Informational Authority: architecture should preserve the differentiated locations of legitimate informational authority unless broader concentration is independently justified.

The principle predates the formal FC architecture. The Utility, Security, Autonomy framework connected individual control with decentralized identity and emphasized delegation, offline alternatives, least disclosure, confidentiality, recourse, and freedom from government surveillance. The later FC work supplied a deeper reason for the design choice. Decentralization is not valuable merely because distributed systems are fashionable or resilient. It is valuable because concentrated informational capability can contradict the distribution of legitimate authority.

This is why technology neutrality does not require neutrality about decentralization. FCGIAS can remain neutral among cryptographic protocols, database products, cloud platforms, credential formats, and implementation techniques while still preferring architectures that do not create unnecessary centralized governmental power.³⁶

The principle must nevertheless be functional. A diagram with ten databases and no central repository can still represent centralized informational power if one service can query all ten, resolve identities, correlate the results, and retain the synthesis. A federated search engine can be a functional data lake. A commercial

³⁶ USA V1 at 1-9. The antecedent framework links Autonomy, individual control, least disclosure, specific purpose, delegation, offline use, and decentralization.

broker can become a reacquisition layer. A universal identifier can make physically separate records trivially joinable. A shared AI service can reconstruct the population profile that purpose sequestration was intended to prevent.

Accordingly, decentralization must be evaluated by effective informational power rather than by network diagram.

No Phone Home provides a concrete example. Consider a government-issued digital credential. The holder presents proof to a verifier. If the verifier contacts the issuer or a central identity provider every time the credential is used, the system may create a new stream of transaction metadata: who presented a credential, when, where, to whom, and potentially for what purpose. The architecture can therefore minimize the attribute disclosed to the verifier while centralizing observation elsewhere.

DHS decentralized-identity requirements recognize the technical problem by seeking to eliminate hidden back channels and phone-home behavior. Fiduciary Commons adds the authority analysis. The issuer's authority to issue or attest a credential does not automatically include authority to observe every subsequent presentation. Verification should therefore be designed, where feasible, so that trust in the credential does not create an unnecessary surveillance relationship.³⁷

The same reasoning applies to the person-held “golden record.” Fiduciary Commons does not seek a government population golden record. Where comprehensive integration is useful to the individual, the individual can often be the locus of integration. A person may hold credentials or records from multiple institutions and present selected proofs for a transaction. A parent may hold credentials for a child. An authorized representative may exercise bounded delegated authority. The integration exists for the person's purposes without creating a standing government-wide profile.

This is not an assertion that every government record should be copied into a personal wallet or that institutional records should disappear. Governments must retain authoritative records for many functions. The architectural point is that convenience for the person does not necessarily require centralized government custody of the person's entire informational life.

Purpose sequestration and decentralized authority are therefore complementary. Purpose sequestration distributes governmental information by legitimate function. Decentralized authority preserves the fact that not every legitimate function belongs to the same actor. No Phone Home prevents a credential infrastructure from recentralizing observability. Authorized Answer allows systems to interoperate without transferring unnecessary substrate. Together they create a form of informational separation.

The analogy to separation of powers should be used with care. The Founders did not design digital identity systems. But Madison's observation that entrusted power may be divided to reduce the risk of betrayal supplies a structural insight. If law distributes authority among institutions, architecture should not casually reverse that distribution by making the separated powers functionally one.

Federalism sharpens the point. Printz and Bond explain a constitutional order in which state and federal governments retain distinct authority and the diffusion of power can protect liberty. Modern data infrastructure can erode that practical separation without formally changing a statute. A shared platform, common identity layer, or universal query service can make records available across jurisdictions in ways that convert cooperation into standing collective capability.

³⁷ U.S. Dep't of Homeland Sec., Silicon Valley Innovation Program, Technical Implementation Requirements for Decentralized Identity: Personal Credential (implementation requirements addressing holder control, selective disclosure, and No Phone Home architecture); VERIFIABLE IDENTITY AND DIGITAL AUTONOMY ACT, Version 2.2 TRI-PATCH-01, §§ 2, 10-13 (Sept. 13, 2026) (Model Act Freeze Candidate) [hereinafter VIDA 2.2].

OIA does not forbid such systems categorically. It asks whether the capability corresponds to an independently legitimate allocation of authority. A congressionally authorized joint program, compact, judicial process, or other lawful mechanism may justify cross-jurisdictional capability. The architecture should represent that basis rather than treating technical interoperability as a source of authority.³⁸

A related principle is provisionally described as Localized Informational Authority. Informational capability should ordinarily remain with the person, program, institution, or jurisdiction closest to the legitimate function for which the authority exists, and should move outward or upward only where broader allocation is independently justified. The idea resembles subsidiarity, but the terminology is intentionally not frozen because “subsidiarity” carries established meanings in federalism, European governance, and other traditions.

The operative point is narrower. Do not centralize informational power merely because centralization reduces administrative friction. Ask first where the legitimate authority resides.

Decentralization also improves the quality of the authorization boundary. In a generalized system, access control often becomes the only barrier between an official and information from unrelated domains. In a decentralized system, a materially broader inquiry may require a new transaction across a trust boundary. That transaction can carry purpose, authority, scope, duration, and audit evidence. Friction, in this sense, can be constitutional information.

Fiduciary Commons does not seek friction for its own sake. It seeks Authorization Friction where materially broader power should require a deliberate transition. Routine legitimate functions should remain efficient. But the architecture should not optimize away every boundary that law or institutional design created to keep power limited.

The strongest objection remains convenience. A centralized platform can make services faster. A common data model can reduce duplication. A universal query fabric can make fraud analysis easier. AI can generate better answers when given broader context. These benefits are real. The response is not to deny them but to apply Least Informational Power: what is the least governmental informational capability sufficient to perform the legitimate function with acceptable reliability, speed, and accountability?

Sometimes the answer will include centralized capability. Sometimes it will include a shared service. Sometimes it will require cross-program data. Decentralized Informational Authority is not a topology mandate. It is a presumption against unnecessary concentration of effective informational power.

That presumption becomes operational through ACCP.

A purpose domain should not be confused with an agency silo. One lawful purpose may span several institutions, and one institution may perform several purposes that should remain informationally distinct. Purpose sequestration follows authority and function rather than organizational charts. The relevant boundary is the legitimate informational relationship, not the location of the server or the name on the office door.³⁹

Authorization Friction must also be calibrated. Administrative friction can burden access to benefits, delay urgent action, and itself impair liberty. FC does not value friction generally. It values a deliberate transition

38 Printz, 521 U.S. at 918-25, 935; Bond, 564 U.S. at 221-23; VIDA 2.2 §§ 2, 14-15, 21. VIDA expressly states that nominal decentralization can recreate generalized informational power through federated search, common identifiers, metadata, APIs, identity resolution, AI, or other functional integration.

39 NIST SP 800-53 Rev. 5, AC-6; NIST SP 800-207, at 4-7; Cavoukian, *supra* note 10; Rosenzweig, *supra* note 13; FCGIAS Version 2.2, Consolidated Controlling Edition (ACCP and AC-delta controls). FC's claimed contribution is the systematic comparison of standing governmental technical capability to standing legitimate informational authority.

when informational power materially expands. Routine transactions within stable authority should be automated and efficient; friction belongs at the boundary where a new justification is legitimately required.

PART VII. ACCP AND THE ARCHITECTURE OF LIMITED INFORMATIONAL POWER

The Authority-Capability Correspondence Principle converts OIA from a jurisprudential theory into an architectural test:

A conforming governmental information architecture should cause government's Standing Technical Informational Capability to correspond to, and not materially exceed, its Necessary Standing Informational Capability, which in turn must remain within Standing Legitimate Informational Authority.

The formulation is deliberately structural. It asks what the system makes possible under ordinary standing conditions. It also deliberately uses “approximate.” Governmental authority is not reducible to a perfectly static technical state, and systems require operational headroom, emergency mechanisms, administration, recovery, and lawful discretion. The test is material correspondence, not mathematical identity.

ACCP has important antecedents. Least privilege seeks to limit access to what is necessary for a function. Zero Trust removes assumptions of trust based on network location and emphasizes per-request authorization. Privacy by Design seeks to embed privacy into systems rather than rely on downstream compliance. Rosenzweig argued more than two decades ago that new surveillance technology should implement existing legal limits rather than become a basis for new governmental powers or capabilities. Fiduciary Commons should acknowledge those contributions directly.

The distinct move is the comparison itself. The left side of ACCP is government's standing technical informational capability. The right side is government's standing legitimate informational authority. The principle asks whether architecture has created a material Authority-Capability Delta.⁴⁰

An Authority-Capability Delta exists when government can, through ordinary permissions and available system functions, obtain materially more individualized knowledge than its standing authority justifies. The delta can arise from broad administrator rights, universal search, reusable APIs, common identifiers, broker subscriptions, unrestricted AI agents, metadata aggregation, dormant but activatable features, or combinations of otherwise bounded systems.

The test is functional. If an official can ask a vendor to perform a query under an ordinary subscription, that capability may matter to governmental conformance even though the vendor is not a governmental fiduciary and even though constitutional state-action analysis would require a separate inquiry. If an AI agent can invoke an API because the service account has permission, the capability exists for conformance purposes even if policy instructs the agent not to use it outside a narrow mission.

This is why structural limits are generally preferable to policy-only limits where feasible. A policy can prohibit misuse. Training can reinforce duties. Logging can deter misconduct. Audit can identify violations. Those controls are valuable, and some discretion can never be engineered away. But when a material capability is unnecessary to ordinary lawful operations, making the capability technically unavailable provides stronger assurance than making it available and promising not to use it.

The preference is rebuttable. Structural limitation can impose cost, reduce resilience, complicate emergency response, or interfere with legitimate discretion. ACCP does not require technical impossibility at any price. It requires government to recognize excess capability as a governance issue rather than treating availability as neutral.

⁴⁰ NIST SP 800-63C-4 §§ 3.11.2, 7.3 & examples (2025); FCGIAS Version 2.2, Consolidated Controlling Edition § 20.

Least Informational Power supplies the design optimization. Traditional minimization often asks how much data is collected or disclosed. Least Informational Power asks how much governmental power to know the architecture creates. The two measures overlap but are not identical.

A system can transfer very little data per transaction while creating powerful longitudinal metadata. It can leave source records untouched while enabling universal search. It can disclose a Boolean answer while logging every verification centrally. It can avoid retaining raw data while an AI service retains embeddings or learned artifacts that preserve materially useful individualized information. Least Informational Power therefore evaluates the effective knowledge and operations available to government, not only the number of fields copied.

Authorized Answer is one of the most practical implementations. Where government is legitimately entitled to an answer, authority to obtain the answer does not automatically entail authority to acquire the entire informational substrate from which the answer can be derived.

An age-verification transaction is the simplest illustration. If law requires a verifier to know whether a person is at least eighteen, a cryptographically verifiable “yes” may satisfy the function without revealing the birth date. A licensing system may need to know whether a credential is valid, not obtain the holder's complete licensing record. A benefits program may need to know whether a defined eligibility condition is satisfied, not ingest every source record used in the calculation. NIST's derived-attribute guidance demonstrates that such designs are technically ordinary rather than speculative.

Authorized Answer is not universal. Government sometimes needs the underlying evidence. An adjudication may require a record for appeal. An audit may require reproducibility. A criminal investigation may lawfully require source evidence. A statute may mandate retention. A person may dispute an automated determination and need access to the basis for it. The principle is therefore conditional: where the legitimate governmental function requires an answer rather than the substrate, do not automatically create authority to acquire the substrate.

This is a public-law rationale for selective disclosure. The technical mechanism minimizes information. ACCP explains why minimization can be a limit on governmental power.

Purpose Particularity and Question Particularity further operationalize ACCP. Purpose Particularity requires the governmental purpose to be defined sufficiently to constrain informational capability. “Fraud prevention” may describe a legitimate mission but still be too broad to justify unrestricted search across every governmental record. “Determine whether this payment is improper under the statutory criteria applicable to this program and identified predicate” is more capable of constraining architecture.

Question Particularity asks what informational proposition government is authorized to resolve. The question may be categorical, such as eligibility. It may be investigative, such as whether specified records corroborate a predicate. It may be relational, such as whether two entities share a legally relevant connection. The architecture should be capable of representing the question rather than treating every authorized purpose as permission to browse the informational environment.⁴¹

The Medicare fraud statutes demonstrate why this distinction matters. Congress has expressly authorized an integrated repository, interagency matching, and predictive analytics for defined program-integrity functions. ACCP does not deny that authority because the capability is broad. It begins with the grant. The conformance inquiry then asks whether the implemented capability tracks the grant or silently becomes a reusable government-wide analytics platform for unrelated functions.

41 31 U.S.C. § 3354; 42 U.S.C. §§ 1320a-7k, 1320a-7m. These authorities demonstrate that broad informational capability can be legitimate when broader authority is affirmatively granted.

The same method applies to emergency powers. If law permits materially broader access during a declared emergency, capability can expand rapidly when the predicate is satisfied. The architecture should record the authority transition, scope the expanded capability, and contract it when the authority ends. Emergency speed is not the same thing as permanent integration.

AI makes the correspondence problem more difficult because capability can be compositional. An agent may possess no database of its own yet be able to call identity, benefits, tax, licensing, geospatial, and commercial services. The aggregate capability of the agent chain can exceed the apparent permissions of any single component. FCGIAS therefore applies boundary inheritance: AI and automated agents inherit the authority boundaries of the governmental function they serve. Computational capacity does not create independent governmental authority.

Learned artifacts also matter. A model, embedding, score, or persistent feature can preserve informational capability even after raw records are deleted or access is withdrawn. ACCP therefore has to evaluate what the system can still infer or reconstruct, not simply whether the original data remains stored.⁴²

Consider an agent used to detect improper payments. During an authorized period it receives benefits, provider, and transaction data and writes persistent entity embeddings into a feature store. The source permissions later expire, but the embeddings continue to encode associations among beneficiaries, providers, addresses, and transaction patterns. A different program then queries the feature store to identify 'high-risk' persons without reopening the original sources. Deleting the raw records from the agent's working context has not necessarily contracted governmental capability. The learned artifact can function as retained derived information and must be evaluated according to the authority for its continued use.

Vendor technology presents a parallel problem. A private vendor does not become a governmental fiduciary merely because it contracts with government. Halleck confirms that contracting, licensing, regulation, funding, or even monopoly status does not by itself make a private entity a state actor. Skinner, Blum, and Lugar show that constitutional attribution can change when government compels, significantly encourages, participates in, or jointly undertakes private conduct. Those doctrines are fact-sensitive and should remain distinct from FCGIAS conformance.

For conformance purposes, the relevant question is simpler: what capability can government actually exercise through ordinary contractual rights, subscriptions, interfaces, service accounts, or requests? If a vendor platform gives government standing access to generalized individualized knowledge, government cannot avoid the ACCP inquiry by locating the computation on a private server. Conformance attribution is not a declaration that the vendor is a fiduciary or state actor. It is an assessment of governmental capability.⁴³

This makes procurement a constitutional and fiduciary implementation point. Government chooses capabilities when it writes requirements, evaluates products, negotiates interfaces, purchases subscriptions, and accepts administrative features. If the acquisition includes universal search, cross-domain identity resolution, broad enrichment, or unrestricted AI access that the governmental function does not require, the Authority-Capability Delta can be created at contract award before any employee misuses the system.

The procurement maxim is therefore: government should procure functions, not generalized informational capability. Existing procurement law already demonstrates that contracts can transmit privacy safeguards,

42 GOVERNMENT ALGORITHMIC ACCOUNTABILITY AND AI FIDUCIARY ACT, Version 2.2 TRI-PATCH-01, §§ 5-6, 9-12, 19, 29 (Sept. 13, 2026) (Model Act Freeze Candidate) [hereinafter GAAFA 2.2]. The draft applies AI Boundary Inheritance and rejects computational capability as an independent source of governmental authority.

43 *Manhattan Cmty. Access Corp. v. Halleck*, 587 U.S. 802, 809-15 (2019); *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614-16 (1989); *Blum v. Yaretsky*, 457 U.S. 991, 1004-12 (1982); *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936-42 (1982). Conformance attribution under FC remains distinct from constitutional state-action attribution.

rules of conduct, security requirements, and government inspection rights. Fiduciary Commons extends the logic to capability itself. Requirements should identify the legitimate function, disclose the capabilities the product creates, prohibit unnecessary generalized access, and make conformance testable.⁴⁴

ACCP ultimately changes the object of system review. Conventional assessment often asks whether the system has adequate controls around the capabilities it contains. ACCP first asks whether the capabilities should be there. That distinction leads to a remediation hierarchy. If excess capability is unnecessary, remove it. If removal is impossible, narrow it. If broad access can be replaced by bounded transactions, transactionalize it. If greater capability is sometimes legitimate, require renewed authorization before activation. Segregate functions where authority is distinct. Use monitoring and audit for the residual discretion that cannot reasonably be eliminated.

The strongest form of conformance is not a promise that government will refrain from using generalized power. It is an architecture in which materially broader power is unavailable until legitimate authority changes.

The principle can now be stated in affirmative rather than defensive terms. Government should be powerful enough to perform every legitimate function assigned to it. It should be able to obtain reliable answers, coordinate services, investigate wrongdoing, respond to emergencies, and use modern computation. But those capabilities should be ordered to the authority that legitimates them.

That is the architecture of limited informational power. The next task is to show how its operational principles behave in concrete governmental transactions and hard cases.

A. Applying ACCP: The Authority-Capability Delta

ACCP can be applied without pretending that law can be translated into a single numerical score. The first step is to define the ordinary authority state. For the governmental function under review, identify the actor or institution, source of authority, legitimate purpose, relevant population or object, informational domains, permitted operations, permissible correlation and inference, duration, disclosure, and consequence. The second step is to define the ordinary technical state using the same dimensions. What can the deployed system, including administrators, service accounts, vendors, APIs, AI agents, subscriptions, and ordinary escalation paths, actually obtain or construct without a new authorization event? The third step is to compare the two states. A material mismatch is an Authority-Capability Delta.⁴⁵

This comparison is qualitative but disciplined. A delta may arise because the system reaches a population the authority does not cover, accesses a domain not justified by the purpose, permits an operation not contemplated by the legal basis, retains active query power after the relevant authority ends, or enables a consequence for which the underlying information was not authorized. It may also arise because several individually permissible functions compose into a capability no actor separately possesses. The conformance question is not whether every field has a matching statutory citation. It is whether the system's effective power remains materially bounded by the authority that legitimates the governmental function.

Materiality in correlation and inference can be assessed through recurring factors. An operation is more likely to be material when it exposes a previously unknown person or relationship; crosses a purpose, program, institutional, or jurisdictional boundary; produces a new sensitive fact, classification, prediction, or

44 48 C.F.R. §§ 24.102, 39.105 (2026); FCGIAS Version 2.2, Consolidated Controlling Edition §§ 93-95. The FAR provisions demonstrate that procurement can transmit privacy and safeguard requirements; FC's rule to procure bounded functions rather than generalized capability is a stronger proposed architectural requirement.

45 FCGIAS Version 2.2, Consolidated Controlling Edition controls CF-01 through CF-17 and the formal conformance sequence; see also FCGIAS Version 2.2, Consolidated Controlling Edition § 99. The main text intentionally states the method at a higher level than the full assessor-facing control catalog.

risk judgment; materially increases the comprehensiveness or persistence of an individualized profile; enables a new governmental consequence; or accomplishes computationally what would have required separate authority had government sought the resulting information directly. No factor is invariably dispositive. The purpose is to distinguish routine computation within an authorized function from an operation that materially enlarges governmental power to know.⁴⁶

The method necessarily retains legal judgment. Statutory terms can be ambiguous, constitutional rules can be contested, and agencies may possess implied authority necessary to carry out express functions. ACCP is not an algorithm for resolving those disputes. It forces the dispute to be identified before architecture silently resolves it in favor of maximum capability. Where authority is uncertain, the system owner should document the legal basis relied upon, the capability enabled, and the institutional actor responsible for the judgment. That evidence makes later review possible and prevents technical availability from masquerading as legal interpretation.

The same method clarifies Structural Least Power. A material delta does not automatically prove illegality, but an avoidable ordinary standing capability that materially exceeds Necessary Standing Informational Capability is a structural defect rather than merely a reason for stronger safeguards. The preferred response is to remove unnecessary power, narrow it, transactionalize it, or make it predicate- and authority-contingent. If operational necessity justifies residual standing capability, that necessity should be explicit and compensating controls should address the residual risk. Such controls do not cure standing capability that could reasonably have been made materially less informationally powerful. Structural Least Power is therefore a rebuttable design rule grounded in limited power, not a claim that every legal boundary can or should be rendered technically impossible.

PART VIII. OPERATIONAL PRINCIPLES

The preceding Parts establish the architecture's governing propositions. Operational conformance requires those propositions to be expressed at the level of an informational act. Fiduciary Commons therefore treats a material governmental information transaction as a bounded movement or exercise of authority rather than as an unstructured use of data. The transaction should identify the governmental actor, the authority invoked, the purpose, the person or object to which the inquiry relates, the informational question or operation, the permitted sources, the duration, the permitted consequence, and the evidence by which the authorization can later be reviewed.

This approach does not require every ordinary database lookup to become a constitutional ceremony. Routine operations can be automated when their authority is stable and well defined. The point is representability. A conforming system should be capable of distinguishing an ordinary authorized transaction from an operation that changes purpose, crosses a domain, expands the population, introduces a new correlation, or produces a materially broader inference. If the architecture cannot represent those differences, it will tend to treat materially different exercises of governmental power as technically equivalent.

Purpose Particularity is the first operational discipline. A purpose such as “public safety,” “fraud,” “customer service,” or “analytics” may be legitimate yet too capacious to constrain a system. A conforming purpose should identify the governmental function closely enough that the permissible information, operations, actors, and endpoint can be derived from it. Purpose is not a slogan attached to access. It is part of the authorization state.

Question Particularity is the second. Government should identify, at an appropriate level of specificity, what it is authorized to resolve. A verifier may ask whether a credential is valid. A benefits program may ask whether defined eligibility conditions are met. A fraud unit may test a specified predicate. An investigator

⁴⁶ PDTA 2.2 §§ 3, 8-10; FCGIAS Version 2.2, Consolidated Controlling Edition controls CF-14, CF-15. The materiality factors in the text are an FC operational synthesis designed to distinguish ordinary processing from authority-bearing expansion.

acting under process may seek identified records or information within the scope of that process. The question supplies a technical object against which minimization and scope can be evaluated.

Authorized Answer follows from Question Particularity. If the legitimate governmental function is satisfied by an answer, architecture should not automatically convert authority to obtain that answer into authority to acquire the entire evidentiary environment. This principle can reduce collection, but its deeper function is to reduce institutional power. It preserves the distinction between being entitled to know that a condition is satisfied and being entitled to possess everything from which the condition can be derived.

Progressive Particularization governs situations in which legitimate inquiry develops over time. An initial predicate may justify a bounded first inquiry. The result may establish grounds for a broader second inquiry. That second inquiry may justify a third. The architecture should permit this progression while requiring the authority state to change when the scope materially changes. Justice Jackson's *Chatrie* concurrence supplies a useful doctrinal analogy: later stages of a geofence process should not become a roving commission merely because an earlier stage was justified. FC generalizes the structural insight without claiming that every administrative progression requires judicial approval.⁴⁷

Correlation and inference require the same treatment. The fact that government may lawfully access two sources does not answer whether it may join them for every purpose. Nor does lawful possession of source data answer whether every materially consequential inference is authorized. The operative question is whether the correlation or inference remains within the authority of the governmental function or creates materially broader individualized knowledge. Where it does the latter, the operation should be represented as an authority-bearing event.

Retention is likewise a capability question. A record retained for audit, adjudication, statutory preservation, or another lawful purpose may be legitimate even after its active operational use ends. But retention authority is not necessarily active query authority. A system can preserve information while making it unavailable for ordinary reuse. This distinction matters because dormant information can otherwise become standing power merely because storage is inexpensive.

Metadata receives no categorical exemption. Time, location, transaction identifiers, issuer-verifier relationships, query histories, and system logs can reveal information about persons and institutional relationships even where content is minimized. Some metadata is indispensable for security, audit, fraud detection, and operations. FC asks whether the metadata collected and the uses made of it are bounded to those purposes rather than becoming a parallel source of generalized knowledge.

Exceptional authority must also be representable. Emergencies, judicial process, national-security authorities, statutory overrides, and other exceptional regimes may legitimately expand governmental power. A conforming architecture should permit that expansion without making the exceptional capability the ordinary baseline. The authority source, scope, duration, actor, and termination condition should be distinguishable, and capability should contract when the exceptional authority ends unless another lawful basis supports continuation.⁴⁸

Finally, audit is evidence, not absolution. Logging can show whether an actor remained within permissions. It can support accountability and deterrence. It cannot cure an architecture whose ordinary permissions themselves create materially excessive power. The operational objective is therefore layered: legitimate authority, appropriately bounded capability, evidence of the authorization state, and audit of actual exercise.

47 *Chatrie*, 609 U.S. ___, slip op. at 1-4 (Jackson, J., concurring); FCGIAS Version 2.2, Consolidated Controlling Edition control CF-19 (Progressive Particularization). The concurrence is an analogy for staged renewed justification, not a holding governing ordinary administration.

48 FCGIAS Version 2.2, Consolidated Controlling Edition §§ 83-86; PDTA 2.2 §§ 8, 18. Exceptional authority changes the authorization state; it does not create a general exception to OIA.

B. Contestability, Remedies, and Exceptional Authority

Structural prevention does not eliminate the need for rights and remedies. A person affected by governmental informational action may need to know that information was used, obtain reasons for a consequential decision, correct inaccurate information, challenge an inference, or seek administrative or judicial review. Existing law supplies these protections unevenly across domains. Model FC legislation can add duties, enforcement by appropriate public officials, and private rights of action where policymakers choose. The architectural principle is that evidence necessary for contestability should be preserved without turning audit data into a new generalized surveillance resource.⁴⁹

Remedies are complementary to architecture, not substitutes for it. A damages action after an impermissible population profile has been constructed does not erase the capability or the institutional knowledge already created. Conversely, technical prevention without review can conceal errors inside automated systems. Ordered informational authority therefore combines *ex ante* capability limits with *ex post* accountability appropriate to the legal regime.

Exceptional authority does not sit outside OIA. It changes the authorization state. An emergency, national-security authority, court order, or other lawful exceptional predicate may justify capabilities that would be impermissible in ordinary administration. FC does not purport in this paper to define the substantive breadth of every such authority. It insists on a structural proposition: exceptional power should have an identifiable source, authorized actors, scope, purpose, duration, and downstream-use rules, and the system should distinguish its activation from ordinary standing authority.

This matters most when emergency architecture persists. Temporary integrations created during a crisis can become convenient permanent infrastructure. An exceptional query permission can migrate into an ordinary administrative role. Data acquired under one authority can become training material or analytic substrate for another function. Continuing conformance therefore asks not only whether the initial emergency access was lawful, but whether the capability and derived informational artifacts contract, segregate, or receive a new lawful basis when the exceptional authority ends.

PART IX. HARD CASES

A theory of informational limited government is credible only if it can survive the cases in which broad knowledge appears most useful. The following examples are not designed to prove that one technical pattern is always correct. They test whether OIA can preserve legitimate governmental effectiveness while resisting unnecessary generalized power.

A. Benefits and No-Wrong-Door Service. Consider a person seeking public assistance. A humane government should not force the person to understand every program boundary or repeatedly submit the same proof. No-wrong-door service can therefore be a legitimate objective. The conventional architectural response is to integrate identity, income, household, disability, residency, and program records so that a portal or caseworker can see the whole person across government. That may improve service, but it can also create a standing population-scale profile available beyond the immediate transaction.

FC asks whether the same service can be produced with less governmental power. A person-centered service could identify programs through bounded eligibility questions, person-held credentials, or program-to-program queries that return authorized answers. Where the person requests broader navigation, that request can supply authority for a defined service transaction. Where law independently authorizes matching, the architecture can execute it. The objective is not to preserve bureaucratic inconvenience. It is to avoid treating seamless service as a sufficient reason to create a permanent citizen-360 capability.

⁴⁹ USA V1 at 7 (Recourse); GAAFA 2.2 §§ 14-18, 39. FC treats contestability and remedies as complements to structural limits rather than substitutes for them.

Supplemental Security Income (SSI) illustrates the distinction. Eligibility depends on defined legal criteria, including income and resources. A system evaluating eligibility may legitimately need reliable evidence concerning those criteria. It does not follow that every program participating in a common portal should possess standing access to every source record used by every other program. The appropriate architecture depends on the governing law, evidentiary needs, appeal rights, and program relationships. The FC question remains constant: what answer or evidence is necessary for this function, and what broader knowledge should require a separate authority state? ⁵⁰

B. Digital Identity and No Phone Home. Digital identity provides the clearest demonstration of Authorized Answer. A verifier may need to know that a person is over a threshold age, holds a valid license, resides in a jurisdiction, or possesses a professional qualification. NIST's derived-attribute model demonstrates that the verifier can sometimes receive a limited assertion rather than the underlying attribute. Selective disclosure therefore reduces unnecessary exposure at the transaction edge.

But selective disclosure alone is insufficient if the architecture creates central observability. If every credential presentation contacts the issuer or identity provider, that actor may learn where and when the credential is used and by whom. A system can thus minimize disclosed content while maximizing behavioral visibility. No Phone Home addresses this failure. Verification should, where technically and legally feasible, occur without creating an unnecessary issuer-verifier surveillance channel. The principle follows from functional decentralization: the issuer's legitimate authority should not silently become standing authority to observe downstream life. ⁵¹

C. Fraud and Program Integrity. Fraud is the strongest challenge to a framework skeptical of generalized capability because patterns often emerge only through correlation. Federal law makes the challenge concrete. Congress has expressly authorized designated database review through the Do Not Pay Initiative. Medicare and Medicaid law authorizes an integrated repository and interagency matching for fraud, waste, and abuse, and separately requires predictive analytics using large datasets, provider networks, billing patterns, and beneficiary-utilization patterns.

These authorities demonstrate why FC is not an anti-integration doctrine. The law can grant broad informational authority for a defined function. Where it does, the architecture may legitimately provide correspondingly broad capability. ACCP then asks whether the capability remains ordered to the grant. Does a Medicare fraud platform become a reusable investigative environment for unrelated tax, licensing, immigration, or law-enforcement purposes? Can analysts expand from the authorized population to other persons without a new basis? Are derived relationships retained and repurposed? Does an AI model trained for fraud become a general government risk engine? The legitimacy of the initial integration does not answer those later questions.

A well-designed fraud architecture can therefore be powerful and bounded. It can use authorized sources, execute authorized correlations, preserve evidence, and support investigation. It can also distinguish exploratory pattern detection from consequential action, require additional predicates before broader individualized inquiry, segregate unrelated domains, and record the authority for expansion. The goal is not to make fraud detection weak. It is to prevent a legitimate anti-fraud capability from becoming generalized governmental knowledge by default. ⁵²

D. AI and Agentic Government. AI intensifies the problem because it can integrate functionally without centralizing physically. An agent can query several systems, call a commercial enrichment service,

⁵⁰ 42 U.S.C. § 1382; 20 C.F.R. § 416.1100. SSI is used only as an eligibility illustration; the text does not imply that SSI presently operates through FC architecture.

⁵¹ NIST SP 800-63C-4 §§ 3.11.2, 7.3 & examples (2025); DHS, Technical Implementation Requirements for Decentralized Identity: Personal Credential; VIDA 2.2 §§ 10-12.

⁵² 31 U.S.C. § 3354(a)-(d); 42 U.S.C. §§ 1320a-7k(a), 1320a-7m(a)-(c).

synthesize results, infer relationships, and recommend action. From the user's perspective the databases remain separate. From the government's perspective the agent may possess a generalized capacity to know.

FC applies boundary inheritance. An AI system serving a governmental function inherits the purpose, authority, jurisdiction, domain, predicate, duration, disclosure, retention, and consequence boundaries of that function. It receives no independent public authority merely because its model can perform an operation. If the human office could not lawfully query a source for the purpose at issue, the AI should not acquire that authority through a service account. If a broader correlation requires renewed authority for the human function, automation does not eliminate that requirement.

Agentic systems also create capability-chain problems. Each tool in a chain may appear individually bounded, yet the combination may produce a broader result. Conformance therefore has to evaluate the composite governmental information transaction, not only component permissions. Learned artifacts, persistent memory, embeddings, and derived scores also require review because they can preserve or recreate informational capability after raw inputs are no longer available.

These four cases reveal a common pattern. Legitimate government often needs coordination, verification, correlation, inference, or rapid access. OIA does not deny the need. It asks whether the architecture supplies the needed capability at the authority boundary rather than constructing the maximum capability first and governing its use afterward. The distinction is the difference between powerful limited government and generalized informational power.⁵³

PART X. VENDORS AND PROCUREMENT

Government increasingly acquires informational capability rather than building it. Cloud platforms, identity services, analytics products, commercial datasets, AI models, case-management systems, fraud tools, and managed services can determine what government is capable of knowing. Procurement is therefore not peripheral to informational constitutionalism. It is one of the places where governmental power is designed.

The legal status of the vendor must remain clear. A private vendor does not become a governmental fiduciary merely because it contracts with government. Nor does every contractor become a constitutional state actor. Halleck rejects that automatic conversion; Skinner, Blum, and Lugar demonstrate that attribution depends on government compulsion, encouragement, participation, joint action, or other established doctrines. FC does not replace those rules.

Conformance attribution is not constitutional state-action attribution. FCGIAS includes capability that government can exercise through ordinary Vendor arrangements because the conformance question concerns governmental effective power. That does not make the Vendor a governmental fiduciary merely by contract, nor does it establish that every Vendor act is attributable to the State for constitutional purposes. Those are separate legal inquiries.⁵⁴

The government's own obligations, however, do not disappear when capability is supplied by contract. If an agency lacks authority to maintain a generalized population query system itself, the mere availability of the same function through a subscription should not answer the authority question. Government cannot convert a limit on its own informational power into a purchasing specification for a private intermediary and thereby treat the resulting capability as legally neutral.

⁵³ Nat'l Inst. of Standards & Tech., Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (2023); GAAFA 2.2 §§ 5-12, 19, 29. NIST AI RMF supplies risk-governance context, not governmental informational authority.

⁵⁴ *Manhattan Cmty. Access Corp. v. Halleck*, 587 U.S. 802, 809-15 (2019); *Skinner v. Ry. Labor Excs.' Ass'n*, 489 U.S. 602, 614-16 (1989); *Blum v. Yaretsky*, 457 U.S. 991, 1004-12 (1982); *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936-42 (1982). FCGIAS conformance attribution asks what capability government can exercise through ordinary arrangements; it does not determine constitutional state action or convert a Vendor into a governmental fiduciary.

This is the principle of Actor-Substitution Non-Circumvention. The actor performing the computation may change without changing the governmental character of the capability available to the agency. For FCGIAS conformance, capability available to government through ordinary contractual rights, interfaces, service accounts, subscriptions, or routine requests is included in the system boundary. This is conformance attribution, not automatic constitutional state-action attribution.

Procurement should therefore begin with function. What governmental outcome is required? What information must be known to achieve it? Which operations are necessary? Which broader features are bundled into the product but unnecessary to the governmental function? Can universal search be disabled? Can identity resolution be purpose-bounded? Can the service return an Authorized Answer? Can metadata be segregated? Can AI tools be restricted to authorized sources? Can administrative privileges be scoped? Can exceptional capability be activated only after a represented authorization event?

The procurement maxim is concise: government should procure functions, not generalized informational capability. This does not mean buying intentionally inferior technology. It means specifying the standing capability reasonably necessary for the legitimate function, keeping that capability within Legitimate Informational Authority, and treating materially broader capability as a design issue requiring a new predicate, renewed authorization, demonstrated necessity, or remediation.

Existing procurement law already transmits public obligations into contracts. Federal rules apply Privacy Act requirements to certain contractor-operated systems of records and require information technology (IT) contracts to address privacy, safeguards, threats, rules of conduct, and government inspection. FC extends the same institutional logic to informational capability. Contracts can require architectural disclosure, prohibit undisclosed correlation or enrichment, define metadata handling, constrain subcontractors, require deletion or capability contraction, preserve audit evidence, and make conformance a condition of acceptance and continued operation.⁵⁵

Capability disclosure is particularly important in commercial products. A government buyer may purchase a narrow application whose platform also includes global search, graph analytics, enrichment, identity resolution, model training, or cross-tenant features. A security questionnaire may reveal how the product is protected without revealing what informational power it gives the customer. Procurement review should therefore include an authority-capability inventory: what can the product enable government to know or infer under ordinary configuration, and which functions can be technically removed or bounded?

Contractual controls remain different from governmental fiduciary duties. The vendor's obligations arise from contract, procurement law, applicable privacy and security statutes, direct statutory duties where imposed, and agency principles where applicable. Government's duty arises from its public authority. This distinction matters because it prevents two errors: relieving government of responsibility by outsourcing, and imposing governmental fiduciary status on private firms merely because they provide tools.

Procurement is also where legacy risk can be arrested. Government may inherit systems with broad capabilities that cannot immediately be redesigned. A conforming acquisition regime can freeze expansion, prohibit new cross-purpose uses, require capability mapping, and make modernization contingent on progressive remediation. The appropriate sequence is structural: remove unnecessary capability where possible, narrow what remains, transactionalize broad access, require renewed authorization for exceptional expansion, segregate distinct functions, and audit residual discretion.

In this sense, procurement becomes a form of constitutional implementation without pretending that procurement officials adjudicate constitutional law. They operationalize the authority boundaries supplied by law and policy. The legal system defines legitimate governmental authority. Procurement determines whether the purchased architecture respects it.

⁵⁵ 48 C.F.R. §§ 24.102, 39.105 (2026); FCGIAS Version 2.2, Consolidated Controlling Edition §§ 93-95.

A. Procurement as a Capability Lifecycle

A capability-aware procurement lifecycle begins before solicitation. The program identifies the governmental function and authority baseline; acquisition staff translate that baseline into capability requirements and prohibitions; offerors disclose material query, correlation, identity-resolution, enrichment, metadata, administrative, and AI capabilities. Before award, the government evaluates whether proposed capability materially exceeds the function's standing authority and whether unnecessary features can be disabled or segregated. Acceptance testing verifies the promised boundaries in the deployed configuration rather than relying solely on product documentation.⁵⁶

Conformance continues after award. Contracts should require notice of material feature changes, new data sources, new model behavior, new administrative functions, or architectural changes that can expand informational power. Material changes trigger reassessment. Renewal should consider accumulated capability, not merely price and performance. Termination and decommissioning should address retained copies, learned artifacts, credentials, logs, subcontractor holdings, and the removal of government access. This lifecycle prevents conformance from becoming a one-time procurement certification that drifts out of date as the service evolves.

PART XI. FROM FCGIAS TO POSITIVE LAW

A theory of informational power is incomplete if it depends upon voluntary architectural virtue. Fiduciary Commons therefore developed reciprocally across jurisprudence, architecture, legislation, conformance, and procurement. The legal instruments do not merely implement a finished technical standard, and the technical standard does not create law. Each exposes defects in the others.

The institutional hierarchy is important. OIA is the general theory of legitimate informational power. Fiduciary Commons is the constitutional and fiduciary governance model. FCGIAS translates those propositions into architectural requirements. Positive law supplies enforceable authority, duties, rights, procedures, and remedies. The Normative Traceability Matrix connects legal and architectural propositions. The Conformance Test Suite evaluates deployed capability. Procurement specifications govern acquisition. Model Acts provide jurisdictional adoption paths.

The legal hierarchy runs downward from delegated and legitimate authority, not upward from the standard. FCGIAS does not independently authorize government to obtain information, create a purpose, expand jurisdiction, or impose a consequence. Version 2.2 makes the distinction explicit: Positive Legal Authority identifies a competent legal source, but Legitimate Informational Authority asks whether the resulting informational power is justified in source and scope by the governmental relationship, function, Originating Informational Purpose, Authorized Object or predicate, information domains, operations, necessity, proportionality where applicable, duration, consequence, accountability, and Purpose Divergence. A technical standard cannot bootstrap substantive law, and positive authorization cannot bootstrap FCGIAS conformance.⁵⁷

The Public Data Trust Act is the principal statutory home for fiduciary informational authority. It translates duties of loyalty, care, confidentiality, purpose limitation, authority non-self-expansion, and related constraints into positive law. The Verifiable Identity and Digital Autonomy Act (VIDA) addresses identity and verification, including decentralized architecture, selective disclosure, functional decentralization, and the problem of issuer observability. The Government Automated and Algorithmic Functions Act (GAAFA)

⁵⁶ FCGIAS Version 2.2, Consolidated Controlling Edition §§ 93-99 and control CF-37 (change management). The project procurement specification further treats capability disclosure, acceptance testing, change notice, continuing conformance, and decommissioning as lifecycle controls.

⁵⁷ PDTA 2.2 §§ 2-10; VIDA 2.2 §§ 2, 5-15; GAAFA 2.2 §§ 2, 4-12. These are Version 2.2 Model Act Freeze Candidates and are cited as proposed positive-law translations, not enacted law.

applies the authority structure to automated and AI systems, including boundary inheritance and limits on computational expansion.

The trilogy is intentionally synchronized. A digital identity transaction may feed an automated eligibility decision; a public-data rule may determine which information the identity or AI system can access; an AI system may generate an inference that becomes a new informational act. Separate statutes that use incompatible definitions of purpose, authority, correlation, inference, or authorized action would recreate the fragmentation the architecture is designed to solve. The shared ontology therefore matters.

At the same time, the instruments must preserve institutional roles. Legislatures make substantive policy choices. Agencies implement within delegated authority. Courts interpret law and adjudicate constitutional limits. Technical standards describe conformance. Auditors test evidence. Procurement officials acquire systems. FCGIAS cannot become a vehicle for unelected technical bodies to create new substantive law through a traceability matrix or control catalog.

This is why conformance is evidence-based. A government should be able to demonstrate the authority for a capability, the purpose and scope represented by the system, the technical boundaries that prevent unauthorized expansion, the transitions by which broader capability becomes available, and the evidence showing that those transitions occurred. Conformance is not a privacy score. Some failures are structural and non-compensable. A universal population search cannot necessarily be redeemed by excellent encryption and annual training.

The FCGIAS conformance method therefore includes structural disqualifiers. A Population Golden Record, universal search, standing cross-purpose AI, policy-only purpose limitation, unbounded administration, capability or authority laundering, purpose laundering, authorization-free material expansion, intergovernmental authority aggregation, hidden functional integration, and government-intermediary reacquisition can each create presumptive nonconformance when they produce generalized standing power inconsistent with authority.⁵⁸

'Population Golden Record' in this usage does not condemn every authoritative registry covering a population. A voter roll, licensing register, tax system, or other population-scale record can be legitimate when bounded to lawful purpose and authority. The disqualifying condition is the construction of a generalized cross-purpose governmental record or equivalent capability that makes materially comprehensive individualized knowledge ordinarily available beyond the authority of the component functions.

The red-team test is intentionally severe: assume everyone follows the rules. Can government, using actual permissions, contracts, subscriptions, interfaces, and capabilities, construct or acquire materially comprehensive cross-purpose individualized knowledge without obtaining materially renewed and sufficiently particular authority? If yes, the architecture has exposed a structural problem. If no, the system has done something important that ordinary policy cannot guarantee: it has made limited informational authority real in the technical environment.

Institutionalization also requires continuing conformance. Architecture changes. Vendors add features. APIs are connected. Models are retrained. New datasets become commercially available. Emergency integrations become permanent. A system that conformed at procurement can drift into generalized capability. Material architecture change should therefore trigger renewed conformance review just as material legal change can alter the authority baseline.

The ultimate objective is not a new compliance bureaucracy. It is a coherent institutional package in which jurisprudence, law, architecture, procurement, and audit answer the same question. What informational

⁵⁸ FCGIAS Version 2.2, Consolidated Controlling Edition §§ 97-99. The Standard identifies non-compensable structural defects and eleven structural disqualifiers, including a Government Population Golden Record, Functional Universal Search, Standing Cross-Purpose AI Access, Policy-Only Purpose Limitation, and Government-Intermediary Reacquisition Architecture.

power is government entitled to possess, and does the deployed system materially exceed it? When those layers align, privacy protection becomes a consequence of limited power rather than a promise layered over unlimited capability.

A. Enforcement Allocation and Regulatory Non-Bootstrap

Institutional enforcement should follow the same separation of roles. Legislatures determine substantive duties, authorities, remedies, and delegations. Executive agencies interpret and implement those rules within their jurisdiction. Chief information officer (CIO), privacy, security, data-governance, and procurement institutions translate them into system requirements without acquiring independent power to enlarge substantive authority. Auditors and conformance assessors test evidence against the governing requirements. Courts decide legal disputes within their jurisdiction. Attorneys general or other designated enforcement bodies exercise powers granted by law. The standard coordinates these institutions; it does not replace them.

59

This allocation is essential to Regulatory Non-Bootstrap. A technical body may discover that a control is difficult to implement or that a broader capability would be useful. That finding can support a proposal to the institution empowered to change the law. It cannot itself become the authority for expansion. Conversely, when law grants broader authority, technical standards should adapt so that the capability can lawfully expand. The architecture is subordinate to legitimate law while remaining capable of exposing when technology has moved beyond it.

Version 2.2 therefore sharpens rather than abandons the original radical proposition. Limited informational government is not achieved merely by requiring officials to cite a legal source before they use powerful systems. The architecture must ask whether the power to know remains faithful to the relationship, function, purpose, and conditions that justify the governmental act. That is the point at which fiduciary theory, OIA, Purpose Particularity, Authorized Answer, Least Informational Power, functional decentralization, Authorization Friction, and ACCP become parts of a single theory rather than a collection of privacy controls.⁶⁰

Procurement becomes a particularly important enforcement point. A Vendor does not become a governmental fiduciary merely by supplying technology. Yet government should not acquire a universal search, graph, identity-resolution, commercial-data, or AI capability merely because a platform bundles it or a broad statute can be cited. Version 2.2 procurement instead requires capability disclosure and comparison of the deployed configuration against the governmental function and Legitimate Informational Authority it is intended to serve. The maxim remains: government should procure functions, not generalized informational power.⁶¹

The institutional consequence is significant. The Version 2.2 Normative Traceability Matrix adds explicit rows for Positive Legal Authority, Legitimate Informational Authority, Citizen-Originated Purpose, Purpose Divergence, Informational Justification, Anti-Abstraction, Positive-Authority Bootstrap, relational multi-person legitimacy, and the separation of conformance from legal validity. The formal test suite adds CF-70 through CF-78 and a twelfth structural disqualifier, Positive-Authority Bootstrap.⁶²

59 FCGIAS Version 2.2, Consolidated Controlling Edition §§ 129-133. The Standard expressly subordinates architectural implementation to legitimate authority and separates legislative, procurement, certification, and jurisprudential development roles.

60 FCGIAS Version 2.2 Candidate Standard Designation and Freeze Record (Sept. 10, 2026); FCGIAS Version 2.2-RC1 Integrated Standard §§ 22-24 (Sept. 10, 2026).

61 FIDUCIARY COMMONS VERSION 2.2, Model Procurement Specification §§ 1-6 (Sept. 11, 2026). Vendor capability is included in conformance assessment without making the Vendor a governmental fiduciary merely by contract.

62 FIDUCIARY COMMONS VERSION 2.2, Master Normative Traceability Matrix T-61 to T-69 (Sept. 11, 2026); FCGIAS Version 2.2 Formal Conformance Test Suite CF-70 to CF-78 and Structural Disqualifier SD-12 (Sept. 11, 2026).

The distinction also requires a rule of institutional humility. FCGIAS is not a court and does not become a source of governmental power merely by declaring a control. A conformance assessment may conclude that a positively authorized capability is inconsistent with OIA without instructing an official to disobey controlling law. Version 2.2 therefore distinguishes lawful and FCGIAS-conforming; lawful but FCGIAS-nonconforming; legal authority disputed or indeterminate; and independently unlawful. The Non-Usurpation Rule preserves democratic lawmaking and judicial review while preventing positive authorization from becoming self-validating inside the architecture.⁶³

This refinement changes ACCP. The correspondence is no longer between technical capability and the maximum informational power that can be defended by pointing to positive law. After IR-01, Standing Legitimate Informational Authority supplies the outer ceiling, Necessary Standing Informational Capability identifies the portion of that authority reasonably required as ordinary standing power, and Standing Technical Informational Capability should correspond to, and not materially exceed, that necessity-bounded capability. The Authority-Capability Delta therefore remains high when a broad statute, regulation, contract, subscription, or platform permission makes generalized capability technically or legally available but the governmental relationship and purpose do not justify ordinary standing access at that breadth.⁶⁴

Fraud and program integrity provide the hardest constructive example. Congress can and does enact affirmative authorities for data matching, improper-payment prevention, integrated data, and predictive analytics. Fiduciary Commons therefore cannot plausibly say that cross-source analysis is inherently illegitimate. The Version 2.2 question is more exacting: what program, population, data sources, predicates, analytical operations, consequences, duration, and oversight did the authority actually justify, and does the deployed standing capability materially exceed that legitimate informational scope? A broad anti-fraud statute can authorize powerful analytics without necessarily authorizing a reusable population-wide governmental intelligence environment.⁶⁵

The corresponding Anti-Abstraction Rule is essential. Government cannot cure Purpose Divergence simply by redescribing the purpose at a higher level of generality. Public safety, fraud prevention, program integrity, citizen services, efficiency, security, modernization, analytics, research, innovation, and data-driven government may describe legitimate governmental concerns, but none standing alone answers who may be known, what question may be asked, which information domains may be used, which operations may be performed, what consequence may follow, how long the authority lasts, or what transition is required before government may know materially more.⁶⁶

The citizen-originated case reveals why this matters. When a person voluntarily approaches government for a nonmandatory license, permit, benefit, credential, service, or status, the person's specific purpose presumptively establishes the originating informational boundary. The application does not become generalized consent to unrelated inquiry, correlation, inference, retention, disclosure, or reuse. Government may still possess independent taxation, regulatory, investigative, enforcement, child-protection, public-health, emergency, judicial, or national-security authority. But those functions must establish their own Legitimate Informational Authority rather than parasitically inherit authority from the person's unrelated voluntary transaction.⁶⁷

63 FCGIAS Version 2.2-RC1 Integrated Standard F-1C, § 20 (Sept. 10, 2026); FCGIAS Version 2.2-RC1 Second Whole-System Adversarial Audit, WSA-02, WSA-15, Cross-Layer Consistency Audit (Sept. 10, 2026).

64 FCGIAS Version 2.2-RC1 Integrated Standard §§ 10-12 (Sept. 10, 2026); FCGIAS Version 2.2 Candidate Standard Designation and Freeze Record (Sept. 10, 2026).

65 See 31 U.S.C. § 3354; 42 U.S.C. §§ 1320a-7k, 1320a-7m. These statutes are used as affirmative-authority counterexamples: they demonstrate that substantial matching and analytics may be lawfully authorized, while leaving the separate FCGIAS question whether the deployed capability remains bounded to the authorized function, population, data, operations, and consequences.

66 FCGIAS Version 2.2-RC1 Integrated Standard § 7 (Sept. 10, 2026); FC-P2.1-SD-01 Amendment Instrument § A11.

Consider a voluntary professional-license renewal. The applicant's purpose justifies identity, qualification, fee, and status checks necessary to adjudicate the renewal. It does not by itself authorize a reusable cross-government profile of the applicant's household, travel, purchases, associations, or unrelated benefits history. If an independently authorized criminal investigation later establishes a sufficient predicate to obtain some of that information, the investigation proceeds on its own authority and necessity. The license transaction neither blocks the investigation nor supplies its authority.

A household benefits application illustrates the relational problem. One applicant may necessarily provide information about a spouse, child, caregiver, or co-resident. The applicant's purpose can justify the relational facts necessary to adjudicate the household claim, but it does not automatically justify consequential profiling of the other person for unrelated programs or enforcement. The informational relationship and consequence must be evaluated for each materially affected person.

AI makes the same boundary visible in computational form. An agency may be authorized to use source records for a defined eligibility or fraud function while lacking sufficient justification to infer a materially different characteristic from those records, such as a health condition, relationship network, or generalized risk score. Predictive utility does not create informational authority, and authorized inputs do not automatically authorize every inference technically obtainable from them.⁶⁸

Version 2.2 operationalizes that insight through Purpose Divergence and four Informational Justification Levels. IJ-1, Purpose-Constitutive, covers informational acts intrinsic to resolving the citizen-originated request or performing a sufficiently particular authority-originated function. IJ-2, Purpose-Protective, covers ancillary acts demonstrably necessary to authenticate, secure, or preserve the integrity of the same transaction or function. IJ-3, Purpose-Divergent, covers a materially different objective, relationship, information domain, operation, consequence, or reusable capability. IJ-4, Purpose-Generalized, covers cross-purpose or population-scale reusable capability justified principally by generalized governmental usefulness and is presumptively nonconforming.⁶⁹

The IJ levels are a structured burden-of-justification device, not a numerical score. Classification should be grounded in observable changes: whether the governmental relationship changes; whether the purpose changes; whether new information domains become available; whether the operation changes from verification to collection, correlation, inference, disclosure, retention, or action; whether the Authorized Object or affected population expands; whether consequences become more severe; whether duration or reusability increases; whether correlation or inference creates materially new knowledge; and whether a materially less informationally powerful Authorized Answer can perform the function. No single factor is dispositive. The factors make the reason for heightened justification inspectable and contestable rather than leaving divergence to intuition.

IR-01 adds an antecedent threshold to that analysis: Structural Least Power. Before government justifies a broader standing capability through IJ-2, IJ-3, or IJ-4, it should ask whether a materially less informationally powerful architecture can reasonably perform the same legitimate function with the required utility, legal effectiveness, reliability, latency, resilience, security, accessibility, and operational continuity. Improved accuracy, convenience, cost, or analytic yield may be relevant to that inquiry, but does not by itself establish

67 FCGIAS Version 2.2-RC1 Integrated Standard §§ 4-6 (Sept. 10, 2026); FC-P2.1-SD-01 Amendment Instrument § A8. Authority-Originated Purposes remain independently available but must establish their own Legitimate Informational Authority.

68 GOVERNMENT ALGORITHMIC ACCOUNTABILITY AND AI FIDUCIARY ACT, Version 2.1-RC4, §§ 19, 24-29 (Sept. 7, 2026) (legislative candidate); FCGIAS Version 2.2-RC1 Integrated Standard § 15 (Sept. 10, 2026). The project treats Material Derived Inference and learned artifacts as authority-bearing informational outputs rather than assuming authorized inputs authorize every computational result.

69 FCGIAS Version 2.2-RC1 Integrated Standard pt. VI (IJ-1 through IJ-4) (Sept. 10, 2026); FC-P2.1-SD-01 Amendment Instrument §§ A9-A10.

that broader standing power is necessary. If the narrower architecture reasonably performs the function, the avoidable broader capability is presumptively nonconforming.⁷⁰

The distinction can be illuminated, but not doctrinally established, by the familiar contrast between deferential and heightened judicial scrutiny. Rational-basis review generally tolerates a wide legislative fit between legitimate ends and chosen means. Strict scrutiny, in the contexts where constitutional doctrine requires it, demands a compelling governmental interest and narrow tailoring. Fiduciary Commons does not import those constitutional tests wholesale into information architecture. It borrows the structural insight that the required justification may become more demanding when government employs a more intrusive or consequential means.⁷¹

Positive Legal Authority asks a conventional legal question: has a constitution, statute, regulation within delegated authority, judicial process, lawful administrative authority, legally cognizable individual authorization, emergency authority, or another competent source authorized the governmental act? Legitimate Informational Authority asks a second question: is the informational power justified in both source and scope by the relationship, function, jurisdiction, Originating Informational Purpose, Authorized Object or predicate, information domains, operations, necessity, proportionality where applicable, duration, permitted consequence, accountability, and degree of Purpose Divergence? The distinction is not a claim that FCGIAS can invalidate legislation. It is a claim about what Fiduciary Commons treats as conforming informational power.⁷²

Where Does Legitimate Informational Authority Come From? LIA is not a free-floating moral judgment assigned to a CIO, assessor, architect, or standards body. Under Fiduciary Commons it is derived from the legally and institutionally cognizable relationship in which government acts: the delegated governmental function and jurisdiction; the citizen-originated purpose or independently authority-originated predicate; the Authorized Object or question; the information domains and operations implicated; necessity and particularity; duration and consequence; and the fiduciary constraint against exploiting entrusted informational power for materially broader ends. These criteria do not make FCGIAS an independent source of law. They define the D3 conformance judgment the framework proposes, while particular applications may also be controlled by D1 positive law or supported by D2 interpretation.⁷³

Democratic Authorization Is Necessary but Not Exhaustive. A democratically accountable legislature ordinarily has the institutional competence to create governmental programs and confer informational authority within constitutional limits. Fiduciary Commons does not deny that competence. It distinguishes four questions that can coincide but need not: whether an enactment is legally valid; whether the resulting exercise is politically legitimate; whether the informational relationship satisfies the fiduciary and limited-government principles FC proposes; and whether the architecture conforms to FCGIAS. A legislature may expressly choose a broad population-scale capability. If the enactment is valid, an FC assessor does not erase

70 FCGIAS Version 2.2, IR-01 Adoption and Freeze Update §§ 3-9 (Sept. 11, 2026); FIDUCIARY COMMONS VERSION 2.2, IR-01 NTM and Conformance Controlled Extension, T-70 and CF-79 (Sept. 11, 2026). Structural Least Power precedes graduated Informational Justification and tests whether materially less informationally powerful architecture can reasonably perform the same legitimate function.

71 Compare *Williamson v. Lee Optical of Oklahoma, Inc.*, 348 U.S. 483, 487-89 (1955) (deferential rational-basis review), with *Adarand Constructors, Inc. v. Peña*, 515 U.S. 200, 227 (1995) (strict scrutiny requires a compelling governmental interest and narrow tailoring for governmental racial classifications). The comparison here is explanatory only; FCGIAS does not claim that current constitutional doctrine generally subjects governmental information architecture to strict scrutiny.

72 FCGIAS Version 2.2-RC1 Integrated Standard pt. III, F-1A to F-1C, §§ 22-24 (Sept. 10, 2026); FC-P2.1-SD-01, Legitimate Informational Authority and Purpose-Divergence Doctrine, Development Record (Sept. 10, 2026). These are Fiduciary Commons D3 propositions unless independently made binding by positive law.

73 FC-P2.1-SD-01, Legitimate Informational Authority and Purpose-Divergence Doctrine, Development Record §§ SD-01A to SD-01H (Sept. 10, 2026); FCGIAS Version 2.2-RC1 Integrated Standard pts. III-VIII (Sept. 10, 2026). The general LIA framework is a Fiduciary Commons D3 proposition unless independently made binding by positive law.

it. The framework instead makes the departure visible, preserves traceability, identifies independently applicable constitutional questions, and recommends structural limits where lawful. This is the function of the Non-Usurpation Rule and Express Democratic Departure.⁷⁴

The claim also must coexist with contrary constitutional authority. *Whalen v. Roe* upheld a state system collecting and storing prescription information while recognizing the privacy concerns created by computerized accumulation, and *NASA v. Nelson* assumed without deciding a constitutional informational-privacy interest while upholding challenged background inquiries. Those cases caution against stating a categorical constitutional prohibition on centralized government information systems. FC's broader capability rule is therefore presented as a D3 architectural and fiduciary synthesis, with any D4 claim that construction of generalized capability itself completes a Fourth Amendment violation kept separate from settled doctrine.⁷⁵

PART XII. BEYOND AUTHORIZATION: WHY THE LEGISLATURE'S PERMISSION IS NOT THE END OF THE INQUIRY

Version 2.1 left one important ambiguity insufficiently resolved. It insisted that technical capability does not create governmental authority and that materially broader power requires materially renewed authorization. But its formulation could still be read to permit a broad positive enactment to supply the entire authority side of ACCP. Version 2.2 closes that gap by distinguishing Positive Legal Authority from Legitimate Informational Authority.⁷⁶

LIMITATIONS AND EMPIRICAL QUESTIONS

FCGIAS is a normative and architectural framework, not an empirical demonstration that every proposed implementation will outperform conventional systems on every operational measure. Material questions remain for deployment research: implementation and migration cost; transaction latency; accessibility and recovery; false positives and false negatives; fraud-loss tradeoffs; emergency activation performance; administrative burden; interoperability at scale; and the security consequences of distributing or transactionalizing capability. The framework's claim is that these variables should be measured against a necessity-bounded architecture rather than assumed to justify generalized standing power. Evidence may show that a broader capability is genuinely necessary for a legitimate function. Where it does, FC should recognize that necessity rather than force an inferior system.

CONCLUSION. ORDERED LIBERTY IN THE INFORMATIONAL STATE

The information age has changed the practical meaning of governmental capacity. A government need not seize papers from a desk or assemble a physical dossier to acquire an intimate picture of a person's life. It can query, correlate, infer, enrich, and automate across systems that remain physically separate. It can obtain commercially available information that public institutions never collected. It can use AI to reconstruct

⁷⁴ FCGIAS Version 2.2-RC1 Integrated Standard F-1A to F-1D and § 20 (Sept. 10, 2026); FCGIAS Version 2.2-RC1 Second Whole-System Audit, WSA-02, WSA-15, WSA-16 (Sept. 10, 2026). The Non-Usurpation and Express Democratic Departure rules preserve the distinction between FC conformance and legal invalidity.

⁷⁵ *Whalen v. Roe*, 429 U.S. 589, 600-05 (1977); *NASA v. Nelson*, 562 U.S. 134, 147-59 (2011). These decisions caution against describing centralized governmental information systems as categorically unconstitutional. FC's broader capability rule is presented as D3, with any architectural Fourth Amendment rule separately classified as proposed D4 development.

⁷⁶ FIDUCIARY COMMONS GOVERNMENT INFORMATION ARCHITECTURE STANDARD VERSION 2.2, Candidate Standard Designation and Freeze Record, substantive change from Version 2.1 (Sept. 10, 2026); FCGIAS Version 2.2-RC1 Integrated Standard §§ 1-2, 10-12 (Sept. 10, 2026).

relationships that no official previously knew. The central problem is therefore no longer only what government has collected. It is what government has made itself capable of knowing.

American public law already contains the resources for taking that question seriously. Governmental power is delegated, bounded, divided, and accountable. The Fourth Amendment's history rejects general warrants and wide-ranging exploratory authority. Modern cases recognize that digital systems can transform the scale and quality of governmental knowledge. Privacy law supplies purpose limitation, necessity, compatibility, and matching controls. Security practice supplies least privilege. Digital identity supplies selective disclosure. Federalism supplies a structural commitment to divided authority. None of these sources alone yields Fiduciary Commons. Together they make its central question difficult to avoid.⁷⁷

Fiduciary Commons argues that informational authority is a species of public authority. Facts concerning persons should not be treated primarily as objects of institutional ownership. The person occupies the primary normative position where personal authority governs. Government that legitimately acquires information acts within a secondary fiduciary relationship grounded in delegated public power. Its authority is real, sometimes coercive, and often indispensable. It is also bounded.

Ordered Informational Authority generalizes the principle. Legitimate informational power should be allocated according to relationship, purpose, jurisdiction, and authority. Many limited authorities should not silently become a generalized governmental power to know. Correlation, inference, observability, commercial reacquisition, and AI can create power even without central storage. Decentralization must therefore be judged by effective informational power, not by topology.

ACCP supplies the architectural test. Government's Standing Technical Informational Capability should not materially exceed Necessary Standing Informational Capability, and that necessary capability must remain within Standing Legitimate Informational Authority. Positive Legal Authority is necessary where applicable, but is not self-validating for Fiduciary Commons conformance. Nor does the outer boundary of legitimate authority automatically justify keeping every potentially legitimate capability permanently available. When both Legitimate Informational Authority and functional necessity materially expand through a legally and substantively sufficient transition, capability may expand. When either contracts, ordinary standing capability should contract.⁷⁸

This approach does not ask government to choose between effectiveness and liberty. It asks government to design effectiveness within legitimate authority. A benefits system can be humane without constructing a permanent citizen-360 profile. A digital credential can be trustworthy without creating an issuer surveillance channel. A fraud system can be analytically powerful when law grants that power without becoming a general-purpose intelligence platform. An AI agent can be useful without acquiring authority its governmental principal does not possess.

The master diagnostic can now be stated more precisely: assume everyone complies. What is the most extensive individualized or relational knowledge government can obtain or construct through ordinary standing capability; what Legitimate Informational Authority establishes the outer boundary of that power; what portion of that capability is actually necessary to perform the legitimate standing function; and what legally and substantively sufficient transition must occur before government becomes capable of knowing materially more?

Limited government in the information age requires an answer not only in law books but in systems. The object is neither maximum privacy nor minimum government. It is ordered liberty: government capable of performing legitimate functions with utility and security, capable of knowing what those functions

⁷⁷ See *Riley*, 573 U.S. at 393-97, 403; *Carpenter*, 585 U.S. at 309-13, 320; *Chatree*, 609 U.S. ___, slip op. at 17-29; 5 U.S.C. § 552a; NIST SP 800-53 Rev. 5, AC-6; *Printz*, 521 U.S. at 918-25; *Bond*, 564 U.S. at 221-23.

⁷⁸ FCGIAS Version 2.2, Consolidated Controlling Edition (ACCP); PDTA 2.2 §§ 2-3, 6, 19. These project sources state the authority-capability correspondence proposition as a normative and architectural rule.

legitimately and necessarily require, structurally constrained from maintaining materially broader ordinary standing power merely because technology makes more possible, and capable of expanding when both the authority and necessity that justify expansion have changed.

ABOUT THE AUTHOR

Michael G. Leahy is an attorney and former Secretary of Information Technology and State Chief Information Officer for Maryland. He also served as President of the National Association of State Chief Information Officers. His work has focused on privacy, digital identity, information governance, procurement, and the relationship between governmental authority and technical architecture. He is the author and principal architect of the Fiduciary Commons framework.