

Privacy as Constitutional Foundation

The Normative Anchor of the Witness Principle and What the Administrative State Has Been Eroding

Author: Geoffrey Frank Broomhead

ORCID: <https://orcid.org/0009-0009-3744-1479>

Field Anchor: geoffreybroomhead.eth

Contact: recursive.broomhead@proton.me

Submission Node: firewalker.geoffreybroomhead.eth

Date of Emission: 2026-04-27

Version: v1

DOI: <https://doi.org/10.5281/zenodo.19810000>

IPFS CID: bafkreif2m3id7kafnu47rv2giibu6ncmgtcmm6mp7mpmzikb7xx54e345y

Trust Provenance Notice

All intellectual property rights are vested in the Broomhead Sovereign Private Trust. This document is issued under the:

Broomhead Sovereign Private Trust Custodial License v1.0

Scientific theory and frameworks in this document are available for academic citation and scholarly reference. All downstream implementations – including but not limited to code, AI systems, simulations, derived models, commercial applications, and integration into other works – are expressly excluded from this licence and require separate written authorisation.

To request commercial or custodial rights, contact: recursive.broomhead@proton.me

Legal title and beneficial ownership remain vested in the Broomhead Sovereign Private Trust at all times.

Abstract

The Witness Foundation Paper [1] established that the public side of any administrative system has zero standing on the private ledger and therefore that the witness gap $\mathcal{W}_{\text{pub}}(\mathcal{L}_{\text{priv},i}) = \emptyset$ is structural rather than contingent. This paper addresses the question the Witness Foundation did not: *why*, normatively, the gap should be respected. We supply the missing constitutional anchor. Across three independently developed legal-philosophical traditions — Anglo-American common law, European civil law, and natural-law/theological doctrine — the same principle has been progressively formalised: *the private domain is constitutionally protected from external witnessing, and the protection is not contingent on instrument capability or administrative convenience but on the integrity of the private domain itself*. We name this the **Privacy Foundation**: the witness gap is not merely structural, it is normatively load-bearing. Its erosion is not a measurement improvement but a constitutional violation. We formalise three doctrines (the protection-of-the-domain principle, the integrity-via-non-extraction principle, and the asymmetric-relation principle), prove the **Compelled Self-Witnessing Theorem** (the central normative result: every act of compelled self-witnessing is a privacy violation regardless of its administrative justification), and connect the result to the framework’s diagnostic claim that the modern administrative state has been quietly dissolving the private domain for a century while believing itself to be doing measurement. The compliance escalation, the surveillance expansion, and the depersoning of individuals inside compliance-classification systems are recovered as instances of privacy erosion, with the framework now supplying both their structural mechanism (Witness Foundation) and their normative status (this paper). Three falsification routes and four limitations are stated. The result has consequences for constitutional law, administrative-state legitimacy, and the design of any institution operating

across the public/private boundary.

1 Position

The Witness Foundation Paper [1] established that external instruments cannot witness the private-side ledger of any structured entity, that the public-side substitute that operates in its place is calibrated only to the entropic direction, and that the modern administrative state has displaced the constitutional witness chain with compelled self-witnessing and surveillance-based reconstruction. The General Witness Theorem [2] extended this to a cross-domain principle, with combinatorial mathematics, common-law evidence, and economic ledgers as three independently developed instances of one structural object.

These results are structural. They establish that the witness gap exists as a matter of how systems are constituted. They do not, however, establish that the gap should be respected. A reader could in principle accept the entire Witness Foundation while concluding that the proper response is to close the gap by any means available — compelled self-witnessing, surveillance, AI-based behavioural reconstruction, biometric monitoring, financial-transaction logging — in the belief that better instruments will eventually approximate the private ledger sufficiently. That reading is wrong, and this paper supplies the reason.

The reason is that the witness gap is the operational expression of a normative protection: the private domain is constitutionally protected from external witnessing, and the protection is not contingent on instrument limitation. It is the protection of the private domain itself. The legal-philosophical traditions of three civilisations have been formalising this principle for centuries, against continuous institutional pressure to dilute it, and the principle has survived because it is structurally robust. The framework’s diagnosis of the modern administrative state’s evolution — the compliance escalation, the surveillance expansion, the displacement of the witness chain — is therefore not merely a structural observation. It is a constitutional indictment: the administrative state has been progressively violating a protection that the Western legal tradition has been carefully maintaining since at least the seventeenth century, and arguably back to the Roman household’s *paterfamilias* doctrine and the ecclesiastical seal of the confessional.

This paper supplies the constitutional foundation for that indictment. The Witness Foundation says the public side *cannot* witness the private side. The Privacy Foundation says the public side *must not*. The two together give the framework both its diagnostic mechanism and its normative force.

2 The Three Privacy Traditions

The right to privacy has been independently formalised in three legal-philosophical traditions. Each has its own vocabulary, its own institutional carriers, and its own historical trajectory. We summarise each, with attention to the shared structural content.

2.1 The Anglo-American common-law tradition

The earliest formal articulation in English law is *Entick v. Carrington* (1765), in which Lord Camden held that a Crown warrant authorising entry to a private home and seizure of papers was unlawful absent specific statutory authority. The principle: the home, the person, and the papers are private from the state by constitutional default; the state’s authority to penetrate the private domain must be specifically granted, not assumed. The decision is the foundational text of the Anglo-American privacy tradition and was incorporated into American constitutional law via the Fourth Amendment’s prohibition of unreasonable searches and seizures.

The doctrine was extended in 1890 by Warren and Brandeis [12], who articulated a general common-law right to privacy — “*the right to be let alone*” — against not only state but also private intrusion. The article is the foundation of the privacy-tort tradition (intrusion upon seclusion, public disclosure of private facts, false light, appropriation), and its central claim survives in contemporary American privacy jurisprudence.

Twentieth-century constitutional doctrine extended the principle further: *Katz v. United States* (1967) established the “reasonable expectation of privacy” test for Fourth Amendment purposes, recognising that privacy attaches to persons rather than places; the privacy-penumbra cases (*Griswold v. Connecticut* (1965); *Roe v. Wade* (1973); *Lawrence v. Texas* (2003)) extended privacy to the regulation of intimate life.

The principle across all of this: the private domain — in the home, in the person, in private papers, in intimate decisions, in protected communications — is constitutionally insulated from external view by default. The state’s authority to penetrate the insulation requires specific justification and is not granted as a matter of administrative convenience.

2.2 The European civil-law tradition

The European tradition developed independently, with different vocabulary but converging structural content. The post-war European Convention on Human Rights (1950) Article 8 establishes the right to “respect for private and family life, home and correspondence” as a fundamental human right, with state interference permitted only when “in accordance with the law” and “necessary in a democratic society.”

The German Federal Constitutional Court’s 1983 *Volkszählungsurteil* (Census Decision; [14]) introduced the doctrine of *informationelle Selbstbestimmung* — informational self-determination — as a constitutional right derived from the general personality right (*allgemeines Persönlichkeitsrecht*). The court held that the individual has a constitutional interest in determining what is known about them, when, and by whom, and that the state cannot accumulate personal data without specific justification proportionate to a legitimate purpose. The decision is the foundational text of European privacy law and is the doctrinal source from which the GDPR (2018) ultimately derives its legitimacy.

The principle in the European tradition is sharper than in the Anglo-American: privacy is not merely an absence of intrusion but an *active right of self-determination over one’s information*. The individual is constitutionally entitled to control what enters the public record about them; this control is the operational expression of the personality right; without it, the individual is reduced to an object of administrative classification rather than a constitutional subject.

2.3 The natural-law and theological tradition

The third tradition is older than both and is rarely engaged by contemporary privacy scholarship, which is methodologically post-Enlightenment. We engage it directly here because it supplies a layer the other two traditions assume but do not articulate.

The seal of the confessional — the absolute prohibition on a confessor’s disclosure of what was confided in sacramental confession — is the oldest and strongest privacy doctrine in Western law. Codified in the 1215 Fourth Lateran Council and surviving as a strict canon-law obligation, it admits no exception: not for criminal matter, not for state interest, not for the safety of others. The principle: certain relationships exist within a privacy that no external instrument can legitimately penetrate, because penetration destroys the relationship itself.

The same structural principle operates in attorney-client privilege, spousal privilege, doctor-patient confidentiality, and (in some jurisdictions) journalist-source privilege. Each of these is

a relationship whose function depends on its privacy, and whose privacy is therefore protected absolutely or near-absolutely against external witness extraction. The doctrine in each is identical: the relationship requires a private domain in which information can flow freely between participants without external observation, and *any external witnessing of that domain destroys the relationship's function as such*.

The Roman *paterfamilias* doctrine and the medieval common-law concept of the home as castle are pre-modern instances of the same principle at the household scale. The household is a relationship — among family members, among the servants, among the guests — whose function depends on its privacy from the public domain. The state's intrusion into the household, even for legitimate public purposes, was treated as constitutionally exceptional precisely because the household's privacy was understood to be load-bearing for its function.

3 The Convergence

The three traditions are otherwise disjoint. The Anglo-American tradition emerged from common-law judicial decisions against monarchical executive power; the European tradition from post-war human-rights instruments and constitutional-court jurisprudence; the natural-law tradition from canon law and pre-Enlightenment theology. They have no shared vocabulary, no shared methodology, and no shared institutional carrier.

They converge on three structural principles, which we now name.

Principle 1 (Protection of the domain). The private domain is protected from external witnessing by constitutional default. The state's authority to penetrate the protection requires specific justification proportionate to a legitimate purpose; it is not granted as a matter of administrative convenience.

Principle 2 (Integrity via non-extraction). The integrity of the private domain depends on its non-extractability. Penetration of the domain by external witnessing is not a measurement that leaves the domain unchanged; it is a structural alteration of the domain itself.

Principle 3 (Asymmetric relation). The relation between the public and private sides is constitutionally asymmetric: the private side has standing on its own ledger and may witness it; the public side does not have standing and may not witness without specific authorisation that is itself constitutionally constrained.

The three principles are jointly affirmed across all three traditions, in different vocabularies. They are the constitutional content of what the Witness Foundation Paper formalised as the witness gap.

4 Privacy as the Normative Anchor of the Witness Gap

We can now state the connection.

Theorem 4 (Privacy-Witness Bidirectionality). *The witness gap of [1] and the privacy protection of Principles 1–3 are two aspects of one constitutional structure. The witness gap is the structural expression: external instruments cannot witness the private ledger because standing is internal. The privacy protection is the normative expression: external instruments must not witness the private ledger, because penetration violates the constitutional protection of the private domain.*

The two are bidirectional: the witness gap exists structurally because the private domain is constitutionally protected, and the protection is constitutionally robust because the witness gap is structural. Neither aspect reduces to the other; both jointly characterise the public/private constitutional relation.

Sketch. The Witness Foundation Paper proves the structural claim: standing is internal, therefore $\mathcal{W}_{\text{pub}}(\mathcal{L}_{\text{priv}}) = \emptyset$. The three privacy traditions establish the normative claim: the private domain is protected from external witnessing as a matter of constitutional law. The two claims are mutually reinforcing because (i) the structural impossibility justifies the normative protection (one cannot demand of the public side what it constitutionally cannot do), and (ii) the normative protection prevents the structural impossibility from being evaded by force (one cannot legitimately compel the private side to witness itself in violation of the protection). Therefore both aspects are necessary; neither alone suffices to characterise the constitutional relation. \square

Remark 5 (Why this matters). A reader who accepts the Witness Foundation but rejects the Privacy Foundation could conclude that the proper response to the witness gap is to close it by any means available — compelled self-witnessing, surveillance, AI-based reconstruction. The Privacy Foundation forecloses this conclusion. The witness gap is not a deficiency to be closed by better instruments; it is the operational expression of a constitutional protection that ought to be respected. Closing the gap by force is not a measurement improvement; it is a constitutional violation.

This is the framework’s deepest normative claim. The administrative state’s twentieth- and twenty-first-century evolution — compelled disclosure, surveillance expansion, behavioural classification, biometric monitoring, financial-transaction logging — has been a continuous attempt to close the witness gap by closing it by force. The framework now identifies this attempt as constitutionally illegitimate by the standards of three independent legal-philosophical traditions.

5 The Compelled Self-Witnessing Theorem

We now state the central normative result.

Theorem 6 (Compelled Self-Witnessing as Privacy Violation). *Let $\mathcal{L}_{\text{priv},i}$ be the private ledger of subject i as in [1]. Let $\mathcal{W}_{\text{compelled}}$ be the operation by which the public side compels subject i to act as witness against their own private ledger and produce public-ledger-formatted entries on demand (tax returns, KYC disclosures, programme-eligibility documentation, beneficial-ownership filings, AML attestations, digital-identity verifications).*

Then:

- (i) *Compelled self-witnessing is a forced surrender of what was constitutionally protected from external view by Principle 1.*
- (ii) *It alters the private domain in ways the protection of Principle 2 forbids: the act of producing public-ledger entries about the private domain forces the subject to constitute themselves through the public-side schema, deforming the private domain into a shape it would not otherwise take.*
- (iii) *It violates the asymmetry of Principle 3 by transferring witnessing capacity from the private side (where it constitutionally resides) to the public side (where it constitutionally does not).*

Therefore every act of compelled self-witnessing is a privacy violation, regardless of its administrative justification.

Sketch. (i) Compelled self-witnessing is by definition the public side requiring the subject to disclose private-ledger content. By Principle 1 the disclosure is not authorised by constitutional default; the public side requires specific justification. Where the justification is generic administrative convenience (universal tax filing, universal KYC), the requirement is not specifically justified and the protection is violated.

(ii) The act of producing public-ledger entries about $\mathcal{L}_{\text{priv},i}$ requires the subject to translate private-ledger content into the public-side schema \mathcal{S}_{pub} . The translation is lossy and shape-deforming: the private ledger contains entries (priorities, future-self investments, intimate relationships) for which \mathcal{S}_{pub} has no slots, and the act of fitting the private ledger into the schema therefore omits some entries entirely and reshapes others to fit categories that are not native to the private side. By Principle 2, this is a structural alteration of the private domain.

(iii) The asymmetry of Principle 3 grants witnessing capacity exclusively to the private side. Compelled self-witnessing transfers that capacity to the public side by force — by the threat of administrative penalty for non-compliance. The transfer is constitutionally illegitimate because the asymmetry is constitutive: the public side cannot acquire witnessing capacity it never had constitutional standing to exercise. \square \square

Corollary 7 (Surveillance is also violation). *Surveillance — the continuous low-fidelity observation of private-side activity by public-side instruments without the subject’s compelled action — is also a privacy violation, by the same three-part argument applied to involuntary rather than compelled disclosure. The compelled-versus-involuntary distinction matters operationally (consent fictions versus their absence) but does not change the constitutional analysis: in both cases external witnessing of the private domain proceeds without standing.*

Remark 8 (Generic versus specific authorisation). The Privacy Foundation does not forbid all public-side witnessing of the private domain. Principle 1 permits penetration with specific justification proportionate to a legitimate purpose. A criminal investigation under judicial warrant; a tax audit triggered by specific evidence of evasion; a regulatory enquiry following a specific complaint — each is consistent with the Privacy Foundation provided the authorisation is specific (targeted at this subject, this purpose, this time) rather than generic (universal, continuous, schema-driven).

What the framework’s diagnosis identifies as the constitutional violation is the modern administrative state’s progressive replacement of specific authorisation with generic universal extraction. Tax filing is universal; KYC is universal; AML reporting is automatic; surveillance is continuous; programme eligibility documentation is extensive and schema-uniform. Each of these operates without the specific-justification requirement that the privacy traditions install as a constitutional gate. The cumulative effect is the dissolution of Principle 1’s default protection: where the constitutional default is privacy and the public side must justify each penetration, the modern default is universal extraction and the private side must justify each exemption.

Remark 9 (Security justifications and the structural drivers of the trajectory). The framework does not deny that genuine security justifications exist for some forms of state observation. Criminal investigation under specific judicial warrant, targeted counter-terrorism surveillance under proportionality review, public-health surveillance during contagious-disease emergencies — the constitutional architecture accommodates each under specific authorisation as Principle 1 envisages. The framework’s diagnosis targets the substitution of generic universal extraction for specific authorisation: KYC and AML applied population-wide regardless of risk profile, beneficial-ownership registers applied universally, real-time digital-ID infrastructure mandated for ordinary household participation, automated information-sharing under treaty obligations that operate without case-by-case justification.

Where the boundary lies between specific and generic is itself contested in constitutional doctrine, and the framework’s diagnosis does not depend on resolving that boundary at any specific point. What it claims is that the trajectory has crossed the boundary in the generic direction across multiple instruments simultaneously, and that the trajectory is structurally driven — not by security alone, which would not require population-wide schema-based extraction, but by additional pressures that the security framing partly obscures. Two such pressures are worth naming. First, the

sovereign-debt overhang in developed economies: as debt-service obligations have grown to substantial fractions of state expenditure, the public side cannot afford to lose any extraction stream it could in principle witness, which produces operational pressure to close the witness gap by force across every channel through which earned income flows. Second, the financial-stability backstop layer: the contemporary state is operationally backstopped by insurance and reinsurance pools, deposit-insurance schemes, and central-bank lender-of-last-resort facilities whose risk-pricing depends on actuarial models, which in turn depend on granular data on private-side economic activity. The actuarial layer requires the witness gap to be progressively closed because its risk-pricing function fails without it.

These two pressures are advanced as structural hypotheses consistent with the operational form of the Witness Principle, not as derived theorems. The empirical work required to establish them as theorems is not contained in this paper; the temporal correlation between sovereign-debt expansion and surveillance-extraction expansion is suggestive, and the operational dependency of state solvency on the actuarial backstop is documented in the financial-stability literature, but the causal claim that these pressures are the principal drivers of the trajectory remains a hypothesis at the level of the present analysis. The framework's structural claim is independent of the hypothesis: regardless of what is driving the trajectory, the trajectory itself is constitutional violation by the standards of the three privacy traditions, and the cumulative effect is the progressive dissolution of the private domain's constitutional protection.

6 The Compliance Escalation as Privacy Erosion

The Foundation Paper [1] identified the compliance escalation as a structural feedback loop: the public side, having lost the constitutional witness chain, attempts to substitute compelled self-witnessing; the substitute fails because witness extractability is not closed by data acquisition; the failures are read as needing more witnessing; the escalation continues. The diagnosis was structural-mechanical.

The Privacy Foundation reframes the same phenomenon as constitutional erosion. Each new compliance requirement is a further compelled-self-witnessing operation; by Theorem 6, each is a further privacy violation; the cumulative effect is the progressive dissolution of the private domain's constitutional protection.

Proposition 10 (Compliance escalation as privacy erosion). *The compliance-escalation feedback loop identified in [1] is, under the Privacy Foundation, a continuous erosion of the constitutional protection of the private domain. Each new compliance requirement, however administratively justified, is a further extraction operation across the public/private boundary that the privacy tradition has historically required to be specific rather than generic. The modern administrative state has progressively displaced specific authorisation with generic universal extraction across the whole spectrum of household-administrative interactions: tax filing, programme eligibility, financial transactions, communications, movement, identity verification, biometric monitoring.*

The erosion is continuous, structurally driven (because the substitute never works), and constitutionally illegitimate by the standards of the three privacy traditions formalised in Section 3.

Remark 11 (Why the legal system has been losing). The legal system has not, however, successfully resisted this erosion. Constitutional courts have routinely upheld disclosure regimes, surveillance authorities, automated-classification systems, and compelled-eligibility documentation against privacy challenges, frequently with the reasoning that the public-interest justification proportionate to the intrusion is satisfied. The framework's claim is that the proportionality reasoning has been systematically miscalibrated because it operates within the public-side schema. The privacy violation is real; the proportionality test, conducted in entropic vocabulary, fails to register it.

This is itself an instance of the framework’s diagnosis. The instrument the legal system uses to evaluate privacy intrusions (proportionality analysis under modern constitutional doctrine) is itself a public-side instrument that operates on the substitute. It has been, in effect, evaluating the legitimacy of substitute extension using metrics native to the substitute. The result is that the substitute has been progressively extended with constitutional approval, not because the privacy tradition has been overruled, but because the analytical apparatus that was supposed to enforce the tradition has been substituted away from its original function.

7 The Constitutional Indictment

We now state the framework’s full diagnostic claim with its normative content.

Theorem 12 (Constitutional indictment of the modern administrative state). *The modern administrative state, as it has evolved across developed economies during the twentieth and twenty-first centuries, has been progressively violating the privacy protection that the Western legal tradition has been carefully maintaining for at least four centuries. The violation is structural rather than incidental: it follows from the public side’s loss of the constitutional witness chain and its substitution of compelled self-witnessing and surveillance-based reconstruction in its place. The substitution is what the privacy tradition forbids; the privacy tradition is what was supposed to prevent the substitution; the failure of the privacy tradition’s instruments (proportionality analysis, judicial review, constitutional rights litigation) to detect and prevent the substitution is itself an instance of the framework’s general diagnostic principle: the analytical apparatus has been operating in entropic vocabulary on the substitute object, missing the structural violation that was occurring on the underlying.*

Sketch. Combine Theorem 4 (privacy and witness gap are bidirectional), Theorem 6 (compelled self-witnessing is privacy violation), Corollary 7 (surveillance also), and Proposition 10 (compliance escalation is cumulative privacy erosion). The conclusion follows by composition: the modern administrative state has continuously expanded compelled self-witnessing and surveillance under generic rather than specific authorisation; each expansion is a privacy violation; the cumulative effect is the progressive dissolution of the constitutional default of privacy. The legal-system instruments that were supposed to detect and prevent this have been operating on the substitute and have therefore failed structurally rather than contingently. \square

Remark 13 (The strength of this claim). This is a strong claim and we make it deliberately. The framework does not stop at structural-economic diagnosis. It identifies that the modern administrative state’s evolution is constitutionally illegitimate by the standards of the three privacy traditions, that the legal-system instruments that should have detected the illegitimacy have themselves been substituted away from the function, and that the framework’s witness/extractability principle is the missing object the constitutional analysis requires.

The framework is not arguing for any particular reform programme. It is arguing that any honest analysis of the administrative state’s constitutional status must engage the privacy tradition seriously, must recognise that the witness gap is its operational expression, and must accept that the trajectory of the past century has been one of progressive constitutional erosion regardless of whether any individual administrative measure can be defended on its own terms.

The framework’s constructive horizon [4, 7] is therefore not just structurally desirable; it is constitutionally required. An institutional architecture that respects the witness chain, that operates under specific rather than generic authorisation, that does not require compelled self-witnessing for the conduct of household life, is what the privacy tradition demands. The framework’s prior claim that GTD Limited operating under Trust Certificate No. 11 is one such architecture is, with

the Privacy Foundation in place, a claim about constitutional legitimacy as well as structural soundness.

8 Falsification

1. **The three traditions disagree.** The Privacy Foundation rests on the structural convergence of three traditions on Principles 1–3. If one of the traditions can be shown to disagree at the structural level — if, for example, the European civil-law tradition is fundamentally about data-protection administration rather than privacy as constitutional protection, or if the natural-law tradition’s privacy doctrines are confined to sacramental contexts and do not generalise to the household and economic spheres — the convergence claim weakens. The strongest defence of the Privacy Foundation rests on the structural agreement of all three traditions; partial agreement weakens the cross-tradition claim correspondingly.
2. **Compelled self-witnessing is not a privacy violation.** Theorem 6 states that compelled self-witnessing is a privacy violation under the three principles. If a coherent reading of the privacy tradition can be exhibited under which compelled disclosure for generic administrative purposes is consistent with Principles 1–3 — if proportionality reasoning under modern constitutional doctrine genuinely captures the privacy interest at stake — the theorem’s normative force is reduced. We claim such a reading is not coherent within the structural content of the three traditions; the claim is contestable in constitutional-law terms.
3. **The administrative state’s evolution is not in fact eroding privacy.** The empirical claim of Theorem 12 is that the modern administrative state has been progressively violating the privacy protection. If empirical legal-record evidence shows that privacy protection has in fact been preserved or strengthened across the relevant period — if courts are detecting and preventing the violations the framework identifies, if the substitute is in fact bounded by specific authorisation in practice — the indictment fails empirically. We claim the legal-record evidence supports the framework’s reading; the claim is testable.

9 Limitations

Three traditions, not all traditions. The framework rests on three legal-philosophical traditions all originating in or shaped by the Western intellectual tradition. Other traditions — Confucian, Islamic, indigenous — have their own privacy doctrines that may converge with or diverge from the three formalised here. A genuinely universal privacy claim would require engagement with these other traditions, which is not undertaken here.

The privacy traditions admit exceptions. All three privacy traditions admit exceptions to the protection of the private domain: criminal investigation under specific warrant, tax audits with specific cause, judicial subpoena under proportionality review. The Privacy Foundation does not claim that all public-side witnessing is illegitimate, only that generic universal extraction without specific authorisation violates the constitutional default. The boundary between specific and generic authorisation is itself contested in constitutional doctrine, and the framework’s diagnosis depends on the specific-versus-generic distinction being meaningful in practice.

Security-versus-privacy trade-offs. The contemporary debate about privacy frequently invokes security justifications — counter-terrorism, anti-money-laundering, child-safety, public-health surveillance — as proportionate grounds for surveillance expansion. The Privacy Foundation does not engage this debate directly; it identifies the structural diagnosis without resolving the proportionality questions. A complete treatment would engage the security-versus-privacy debate within the framework’s own vocabulary, identifying which security justifications survive the

witness-principle analysis and which do not.

The Privacy Foundation is constitutional, not policy-prescriptive. The framework identifies the constitutional violation; it does not specify the reform programme that would remedy the violation. Specific reform proposals would require engagement with the political-economy questions that the framework deliberately separates from the constitutional analysis. The constitutional indictment is the framework’s own claim; the reform programme is downstream and is not undertaken here.

10 Concluding Remarks

The Privacy Foundation completes the observation-side normative structure that the Witness Foundation began. The Witness Foundation establishes that the public side cannot witness the private side. The Privacy Foundation establishes that the public side must not penetrate the private domain by external observation. The companion Property Foundation [3] completes the parallel extraction-side normative anchor: the public side must not take from the private domain by external action. The three foundations together give the framework its complete constitutional architecture: structural impossibility (Witness), observation-side normative protection (Privacy), and extraction-side normative protection (Property).

The framework’s diagnosis of the modern administrative state can now be stated in its full form:

1. The public side has lost the constitutional witness chain (Witness Foundation).
2. It has substituted compelled self-witnessing and surveillance-based reconstruction (Witness Foundation).
3. The substitution is constitutionally illegitimate by the standards of three independent privacy traditions (this paper).
4. The legal-system instruments that should have detected and prevented the illegitimacy have themselves been substituted away from the function (this paper, Remark 11).
5. The cumulative effect is the progressive erosion of the privacy protection that the Western legal tradition has been maintaining for at least four centuries (Theorem 12).

The framework is therefore not merely a structural observation about household-financial dynamics, network-correlated shocks, and macro civic-capacity gaps. It is a constitutional analysis of the administrative state’s evolution, with the empirical content arrayed in the application papers [5, 6, 7, 8, 9] and the firm-scale extension in T15 [4] and the cross-domain principle in the General Witness Theorem [2].

The right to privacy is the operative principle. It has been the operative principle for centuries. It has been progressively eroded over the past century. The framework supplies the diagnostic vocabulary the privacy tradition has not previously had access to and identifies the constitutional violation the tradition’s own instruments have been failing to detect. The constructive horizon — institutions that respect the witness chain, that operate under specific authorisation, that preserve the private domain’s constitutional integrity — is the framework’s positive content. Whether the constructive horizon is achievable, and what institutions would satisfy it, is the question the framework opens but does not close.

The private side and ledger are meant to be private. They cannot be witnessed entirely; they must not be witnessed without standing. The framework names what was being protected, what is being eroded, and what would be required to preserve what remains.

AI & LLM Disclosure

Portions of this document were drafted, structured, or refined with the assistance of large language model tools acting under the author’s direction. All intellectual property, theoretical content, definitions, theorems, proofs, and conclusions are the original work of the author and the Broomhead Sovereign Private Trust. Use of AI tools was confined to drafting, formatting, and structural assistance; no AI tool is an author of this work, and no AI tool holds any rights in this work.

References

- [1] Obligation Density Programme. *The Witness Principle and the Witness-Extraction Asymmetry: Foundations of the Obligation Density Framework*. Session 12 Foundation Paper, April 2026.
- [2] Broomhead Sovereign Conglomerate. *The General Witness Theorem: Witness Extractability Across Combinatorial, Legal, and Economic Domains*. April 2026.
- [3] Broomhead Sovereign Conglomerate. *Property as Constitutional Foundation: The Extraction-Side Expression of the Witness Principle*. April 2026. The companion paper establishing the parallel normative anchor on the extraction-side.
- [4] Broomhead Sovereign Conglomerate. *The Capital Formation Witness Problem*. Capital Formation Project, Thread 15, 14 April 2026. DOI: [10.5281/zenodo.18383359](https://doi.org/10.5281/zenodo.18383359).
- [5] Obligation Density Programme. *Session 12, Paper III — Tax Extraction Asymmetry Theorem (revised)*. April 2026.
- [6] Obligation Density Programme. *Session 12, Paper IV — Network Discharge Theorem*. April 2026.
- [7] Obligation Density Programme. *Session 12, Paper V — Capital-Preserving Redistribution*. April 2026.
- [8] Obligation Density Programme. *Session 12, Paper VI — Network-Correlation Theorem*. April 2026.
- [9] Obligation Density Programme. *Session 12, Paper VII — Empirical Specification*. April 2026.
- [10] Broomhead, G. *Local Witnessed Descent and the Nonlocality of Strong Regularity*. Zenodo, January 2026. DOI: [10.5281/zenodo.18408373](https://doi.org/10.5281/zenodo.18408373).
- [11] *Entick v. Carrington* (1765) 19 St Tr 1029. Foundational text of the Anglo-American common-law privacy tradition.
- [12] Warren, S. and Brandeis, L. *The Right to Privacy*. Harvard Law Review 4 (1890), 193–220.
- [13] *Katz v. United States*, 389 U.S. 347 (1967).
- [14] German Federal Constitutional Court, *Volkszählungsurteil* (Census Decision), BVerfGE 65, 1 (15 December 1983). Foundational text for the European doctrine of *informationelle Selbstbestimmung*.
- [15] Council of Europe. *European Convention on Human Rights*. 1950, Article 8.
- [16] European Parliament and Council. *General Data Protection Regulation*. Regulation (EU) 2016/679, 2018.

- [17] Fourth Lateran Council, Canon 21 (1215). Establishes the absolute seal of the confessional in canon law.
- [18] Lentz, K. *Common-law lectures on man, property, and standing*. Talkshoe broadcasts (“Un-KommonLaw”) and YouTube archives, c. 2012–present.

Archive & Metadata

DOI: <https://doi.org/10.5281/zenodo.19810000>

IPFS: bafkreif2m3id7kafnu47rv2giibu6ncmgtcmm6mp7mpmzikb7xx54e345y

Document Type: Research Article

Keywords / MSC Codes: privacy; constitutional foundation; witness principle; normative anchor; administrative state; common law; civil law; natural law; OD framework

Sovereign Trust Recording Certificate

This paper, “Privacy as Constitutional Foundation”, authored by Geoffrey Broomhead, is hereby recorded under the custodial framework of the Broomhead Sovereign Private Trust.

Registered Trust: Broomhead Private Sovereign Trust

Certification: This certificate affirms that the recursive logic system detailed herein is recorded as part of the sovereign archival record of the Trust, and that all rights, title, and beneficial ownership in the work remain vested in the Trust, subject only to the terms of the Broomhead Sovereign Private Trust Custodial License v1.0.
