KSTARR Enterprises, LLC

Negligent Delegation of Digital Enforcement by Sovereign Governments™

How Constitutional Authority Was Quietly Outsourced to Private Platforms

By Legal Theorists **Katherine Starr™**

I. Introduction

The doctrine of **Negligent Delegation of Digital Enforcement by Sovereign Governments™** asserts that when a government relinquishes core public enforcement duties to private, unregulated digital actors, it commits a structural violation of its constitutional and democratic obligations. This delegation is not an incidental policy shift nor a benign administrative convenience; it represents a foundational breach of public trust. Sovereign enforcement is not a service to be outsourced[1]; it is the defining feature of lawful governance. When a state allows unaccountable platforms to determine identity, control access, interpret legal thresholds, and apply punishment without due process, it effectively dissolves the distinction between public authority and corporate[2].

It is essential to distinguish between **regulatory partnerships**, which maintain governmental oversight and judicial remedy, and **enforcement delegation**, which abdicates sovereign responsibility entirely. A regulatory framework may permit a technology company to report suspected activity to authorities. That is cooperation. But when a sovereign government requires the use of platform-run systems to verify age, enforce speech codes, track location, or administer biometric gates, and does so without transparent legal process or public challenge, that is enforcement delegation. And once this enforcement becomes embedded in opaque Terms of Service, proprietary AI filters, or cloud contracts, the very possibility of constitutional remedy is foreclosed.

This framework is the logical and necessary evolution of the digital harm doctrine. Earlier frameworks addressed how platforms create injury through design (Negligent Digital Architecture™[3]), access (Negligent Digital Access™[4]), and code-based governance. But the current harm is no longer isolated to the platforms themselves. It is now **state-enabled**, **legally sanctioned**, and often **internationally coordinated**. Governments across the Western world have not only failed to prevent this privatization of enforcement, they have actively constructed it. This doctrine names that complicity, and it restores the principle that **sovereign enforcement must remain public, lawful, and visible**, no matter how advanced the digital interface.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

This doctrine builds upon and extends the *Digital Maritime Doctrine*™[5], which established that local and regional governments retain enforceable duties to maintain lawful digital passage and protect individual rights in networked spaces. While that doctrine addressed jurisdictional accountability in local digital governance, *Negligent Delegation of Digital Enforcement by Sovereign Governments*™ escalates the claim to the national and transnational level. Together, these frameworks form a comprehensive legal map to restore accountability in a digitally governed world.

II. Legal Foundations of Sovereign Duty

The legitimacy of any sovereign government rests on its exclusive authority to enforce the law within its jurisdiction, and its obligation to do so in a manner that is visible, accountable, and reviewable under the rule of law[6]. In the United States, this principle is embedded in the **separation of powers**, the **non-delegation doctrine**, and the **guarantee of due process** under the Fifth and Fourteenth Amendments. Enforcement of laws, whether related to speech, identity, child protection, or access to public goods, must occur through constitutionally sanctioned mechanisms, not outsourced protocols or platform-authored terms.

Under international legal frameworks, including the **International Covenant on Civil and Political Rights (ICCPR)**[7], to which the United States and most Western democracies are signatories, states bear affirmative obligations to protect the rights to privacy, free expression, legal remedy, and non-discrimination. These obligations cannot be transferred to third parties, especially not to unaccountable private actors, without breaching the treaty's spirit and legal effect. When a sovereign state requires its citizens to pass through privatized filters of compliance in order to access digital speech, verify their age, or participate in public services, it silently delegates enforcement without legal transparency or remedy. This delegation amounts to a systemic denial of the state's obligations under both constitutional and international law.

Critically, the **non-delegation doctrine**[8] exists to prevent precisely this kind of dilution of power. The doctrine holds that core functions of government, especially enforcement, must not be transferred to private entities without clear statutory authorization, limitations, and judicial review. Yet governments have increasingly structured enforcement duties to *appear* as private action while *functioning* as state-imposed control. This structural maneuver circumvents due process, evades constitutional challenge, and obscures lines of accountability. In practice, it means that a citizen's right to challenge unlawful enforcement vanishes, not because the harm didn't occur, but because the actor implementing it was "not the government."

The result is a regime of governance where the **form of democracy is retained**, but its **function is quietly privatized**. A sovereign duty is not fulfilled merely by setting legal objectives; it is only fulfilled when the process for achieving those objectives is **public, accessible, and legally reviewable**[9]. Delegating enforcement to commercial platforms without these safeguards violates the very foundations of lawful sovereignty.

III. Structural Forms of Delegation

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

Sovereign governments across the Western world have quietly embedded private enforcement mechanisms into the daily lives of their citizens. These forms of delegation are rarely acknowledged as such. Instead, they are framed as technological efficiencies, partnerships, or safety measures. But when a citizen's legal eligibility, access, or speech is determined by an algorithm or corporate term of service, without public visibility, legal recourse, or government accountability, that is no longer regulation. It is the privatization of enforcement, and it carries constitutional consequences.

One of the most glaring examples is the **outsourcing of identity enforcement** to private age-verification platforms under the guise of child protection. Laws such as Louisiana's HB 142[10] require adult websites to verify users' ages yet provide no state-run infrastructure for this process. Instead, the duty is delegated to third-party vendors, many of which collect sensitive identity documentation, including government IDs and biometric scans, without public oversight[11]. These systems often fall under Know Your Customer (KYC) standards borrowed from financial regulation, repurposed to restrict access to protected speech. The state compels compliance, but the *enforcement*, and the attendant data harvesting, is entirely privatized.

Similarly, **speech governance has been delegated to platform Terms of Service**, which now function as de facto law[12]. Governments routinely pressure platforms to moderate content, flag disinformation, suppress "harmful" speech, or limit visibility of dissent. In doing so, the state uses private actors to apply coercive force where constitutional protections would otherwise limit governmental interference. Content removed for violating a platform's rules often corresponds with government-endorsed categories, creating a hybrid form of censorship that evades First Amendment scrutiny while delivering the same result: speech is silenced, and no legal remedy is available.

The **education sector** has become a particularly high-risk zone for digital delegation. Entire school systems operate through platforms such as Google Classroom and Microsoft 365[13] Education, which collect extensive behavioral, biometric, and emotional data on minors. In many cases, participation in these systems is mandatory, and students are surveilled through facial recognition, keystroke tracking, and interaction analytics, all managed by corporate software. The sovereign duty to protect children and deliver public education is now executed through commercial code, with little transparency about how the data is used, stored, or monetized.

Even **public services like unemployment, welfare, or healthcare enrollment** have migrated into **cloud infrastructures operated by private vendors[14]**, where access is conditioned on acceptance of opaque digital terms, and eligibility is determined by algorithmic thresholds. These systems often monitor user behavior, browser metadata, and login patterns, treating citizens as data sources rather than legal subjects. In doing so, the state not only surrenders control, it renders enforcement invisible and unaccountable.

Finally, the use of **biometric data for identity confirmation**, whether for accessing government buildings, mobile apps, or national ID systems, has been widely delegated to third-party platforms. Citizens are routinely asked to scan fingerprints, faces, or voices into systems

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

managed by vendors under contract. These processes lack judicial oversight, uniform standards, or opt-out protections. The biometric profile becomes both gatekeeper and enforcer, operating through private code but backed by public mandate.

These structural forms of delegation are not neutral. They represent a profound shift in how law is applied, rights are accessed, and sovereignty is exercised. Behind the interface lies an abdication of duty, and an invisible infrastructure of enforcement that citizens neither see nor control.

IV. Case Studies and Examples

Across jurisdictions, governments have adopted enforcement models that depend not on public agencies but on commercial platforms and third-party systems. This is not anecdotal, it is systemic. The following examples illustrate how sovereign governments have delegated core enforcement functions to private actors under the banner of modernization, safety, or convenience, all while evading traditional legal responsibilities.

In the **United States**, the Executive Branch has increasingly relied on Big Tech platforms to handle identity, access, and digital compliance[15]. Federal agencies, including the IRS and SSA, have contracted with private vendors for digital identity verification, including facial recognition tools operated by third parties. In some cases, citizens must scan their faces or submit biometric data through commercial interfaces, before being allowed to access their own government accounts. These partnerships are often executed through procurement mechanisms or digital modernization initiatives that obscure their constitutional implications. The enforcement is real: no scan, no service. But the actor applying that threshold is not the state, it is a for-profit entity, shielded from constitutional challenge.

The **European Union's Digital Services Act (DSA)** codifies platform co-regulation as a legal norm. Under the DSA[16], large platforms are tasked with identifying, moderating, and reporting "illegal content," but the standards remain vague, the processes opaque, and the oversight mechanisms weak. The burden of enforcement falls not on law enforcement or public bodies, but on platform moderators and automated detection tools. While the DSA imposes certain transparency obligations, the underlying premise remains: the state no longer enforces its own laws directly. Instead, it builds an apparatus of delegated enforcement where platforms serve as quasi-governmental actors, without public legitimacy, judicial accountability, or the ability to appeal.

During the **COVID-19 pandemic**, governments around the world introduced health passports and digital check-in systems that quickly became enforcement gateways[17]. These tools, often developed by third-party vendors, determined whether individuals could travel, work, or enter public spaces. In most cases, there was no meaningful way to challenge a denial or error, and the criteria for access were coded into proprietary systems. Citizens were forced to submit to privately administered biometric or medical verification procedures, with enforcement outsourced to scanning apps and digital databases. The infrastructure of public health

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

enforcement was transferred from sovereign control to platform-based systems, with little or no democratic oversight.

In the context of **smart cities**, enforcement has taken on an even more diffuse and automated form. Municipalities in **Canada, the United Kingdom, and Australia** have deployed sensor networks, surveillance cameras, and predictive policing tools that are operated and maintained by private contractors[18]. These systems monitor everything from pedestrian flow to license plate data to energy usage, often in real time. When violations are detected, such as zoning breaches, unauthorized gatherings, or behavioral anomalies, enforcement actions are triggered automatically or flagged by third-party analysts. Public enforcement becomes automated enforcement, with governments acting more as clients than as constitutional authorities.

Each of these case studies reveals a common pattern: governments construct legal mandates, then **delegate their execution to private infrastructure**. In doing so, they bypass procedural safeguards, deflect responsibility, and erode the very concept of public enforcement. The result is a shadow governance system, technically efficient, legally obscure, and democratically illegitimate.

Additional examples include **long-term government contracts with Microsoft and Amazon Web Services (AWS)[19]** across both defense and education sectors. These tech giants now operate cloud infrastructure that hosts not only classified defense data but also student behavioral records, disciplinary actions, and educational compliance metrics. School districts and federal agencies rely on these platforms to monitor attendance, flag behavioral anomalies, and automate interventions, creating digital profiles of individuals over time. In the defense context, Microsoft's JEDI and Azure Government contracts allow private codebases to mediate sensitive national security decisions, often with predictive analytics and AI modeling that lack public visibility. The enforcement of both discipline and access, whether in a school system or a defense protocol, is no longer handled within a chain of sovereign command, but filtered through corporate logic and proprietary systems. The delegation here is not only widespread, it is foundational to modern state function.

V. Harm to the Constitutional Order

The harm caused by sovereign delegation of digital enforcement is not abstract, it is structural, cumulative, and corrosive to the very basis of constitutional governance. When the power to restrict, verify, surveil, or deny a citizen's access to rights is transferred to unaccountable corporate systems, the citizen's relationship to the state is fundamentally altered. The public no longer engages with a government bound by legal limits, procedural transparency, or judicial recourse. Instead, they are subject to enforcement by algorithmic proxies, data brokers, and platform moderators, none of whom are answerable to the Constitution or any public charter.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

This is not merely a crisis of privacy. It is a collapse of legal remedy and democratic accountability. Citizens who are flagged, suspended, denied access, or surveilled by private systems acting under government mandate often have no means of appeal. But constitutional obligations do not evaporate through outsourcing. As the Supreme Court affirmed in *West v. Atkins*[20], when a private actor performs a public function under state contract or authority, they act "under color of state law" and the state remains liable for the resulting harm. Today, however, platforms point to state mandates while the state defers to platform terms of service. Enforcement floats in a jurisdictional void, everywhere and nowhere. The citizen, meanwhile, loses the procedural protections that once defined the difference between law and coercion.

The constitutional order depends on clearly delineated powers. Legislative bodies make the law; the executive enforces it; and the judiciary interprets its application and constitutionality. This balance of power is disrupted when enforcement is farmed out to opaque third-party systems[21]. The government no longer enforces law through visible institutional processes, it enforces through data filters, platform conditions, and biometric checkpoints administered by non-state actors. In this model, **enforcement is no longer subject to public challenge**, because it is no longer recognized as state action.

This deterioration of the constitutional order is especially dangerous in the digital realm, where enforcement is often **invisible**, **instantaneous**, and **non-reviewable**. Digital enforcement operates in the shadows of code, metadata, and algorithmic flags, erasing the procedural steps through which traditional enforcement was once made legible to the public. What was once the domain of judges, officers, and public hearings is now handled through automated scorecards, platform logic, and third-party verification systems, inaccessible to those they govern.

Moreover, this delegation erodes public trust. When citizens see their governments hiding behind private contracts, disavowing responsibility for harm, or enforcing law through commercially incentivized systems, they lose faith in both the rule of law and the legitimacy of the democratic state. Delegation thus leads not only to individual rights violations but to systemic illegitimacy, a slow unraveling of the public mandate to govern at all.

To maintain constitutional integrity in the digital age, enforcement must remain public, visible, and subject to legal remedy[22]. Delegation, in its current form, threatens all three pillars. And where enforcement collapses into private code, so too does the promise of democratic sovereignty[23].

VI. Legal Theory of Negligent Delegation

The legal foundation of **Negligent Delegation of Digital Enforcement by Sovereign Governments™** rests on the premise that enforcement is a **non-transferable function** of sovereignty. It is not a commodity to be licensed, contracted, or privatized without consequence. When a government enacts law but delegates its enforcement to a private actor who is not accountable to the Constitution, it creates a **negligent breach of public duty**. This breach is not merely administrative; it is legally actionable.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

Negligent Delegation[24] occurs when three conditions are met:

1. The **government imposes a legal obligation** on its citizens (e.g., age verification, speech moderation, biometric access);
2. The **government fails to execute that obligation directly**, instead outsourcing enforcement to a private, unregulated entity;
3. The **citizen experiences harm**, through data exposure, censorship, access denial, or rights restriction, with no viable legal remedy due to the state's displacement of responsibility.

This model is grounded in traditional tort principles of **duty, breach, causation, and harm[25]**, applied to the digital sphere. The state has a **non-delegable duty** to enforce its laws in a manner that upholds constitutional rights and ensures judicial recourse. Delegating that function without providing oversight, remedy, or transparency constitutes a breach. When that breach results in harm, whether in the form of blocked access to services, unwarranted surveillance, or compelled data surrender, it becomes a tortious injury traceable to the sovereign.

Importantly, this framework also implicates constitutional doctrines beyond tort law. The **non-delegation doctrine[2627]**, established in U.S. jurisprudence, prohibits Congress from assigning its core legislative responsibilities to non-governmental actors without clear guidelines. A parallel logic applies to enforcement: if the act of governing includes not just writing but enforcing laws, then transferring enforcement to private entities without oversight is a violation of both separation of powers and due process[28].

Moreover, enforcement via platform code or commercial terms, where no public official is involved, and no appeal mechanism exists, undermines **the procedural guarantees of the Fifth[29] and Fourteenth Amendments[3031]**, as well as the international human rights obligations that demand legal remedy for state-imposed restrictions. When a child is denied access to education through a commercial ed-tech login, or a user is censored from digital speech platforms under state-backed moderation rules, the harm is not merely technical, it is constitutional.

This doctrine does not argue that governments may never work with private vendors. It argues that **enforcement cannot be ceded without consequence**. Delegation without remedy is abdication. And where enforcement occurs without visibility, consent, or legal process, it is presumptively unlawful.

VII. Remedy

To restore constitutional order and reaffirm the public nature of law enforcement, courts must recognize the delegation of digital enforcement to private actors as a **justiciable legal harm[32]**. The remedy must match the structural scale of the violation. This is not a question of individual overreach, it is a systemic breach of duty that requires **judicial, legislative, and constitutional correction**.

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

First, courts must be willing to **pierce the veil of privatized enforcement**. Where a platform, app, or third-party vendor performs a state-mandated task, such as verifying identity, limiting access, or enforcing digital restrictions, it must be treated as a **state actor**[3334] for the purposes of constitutional scrutiny. This allows due process claims, First Amendment challenges, and equal protection arguments to move forward even when the immediate harm appears to originate from a private interface.

Second, governments must be required to **retain sovereign enforcement authority** over all laws that restrict fundamental rights[35]. This does not preclude the use of technology. But it does prohibit enforcement systems where there is no state oversight, no appeals process, and no pathway for judicial review. The use of third-party platforms must come with enforceable public standards, binding transparency obligations, and statutory remedies for wrongful denial or harm. **If the enforcement cannot be challenged, it is not lawful.**

Third, legislation that compels or induces platform-based enforcement, whether through funding incentives, regulatory avoidance, or legal threats, must be subjected to **strict scrutiny**. Laws that displace enforcement from public hands into algorithmic or corporate systems should be presumed unconstitutional unless the state can demonstrate that the process remains visible, appealable, and compliant with procedural safeguards. In this sense, the doctrine functions not merely as a tort framework, but as a **constitutional shield** against state-complicit harm.

Finally, international human rights bodies must hold sovereign governments accountable when digital enforcement mechanisms violate treaty obligations. The **right to legal remedy, to freedom of expression, and to non-discriminatory access to public services** cannot be overridden by vendor contracts or digital protocols[36]. Where international law applies, as it does through the ICCPR[37] and other instruments, sovereign states remain bound, even when the harm flows through code.

This doctrine provides a clear legal blueprint for both litigation and reform. Whether brought as a constitutional claim, a tortious harm, or a statutory violation, **the delegation of enforcement to private digital actors is not benign**. It is a breach of sovereign responsibility, and it must be treated as such by the courts.

VIII. Application

The doctrine of *Negligent Delegation of Digital Enforcement by Sovereign Governments*™ is not theoretical, it provides an immediate, actionable framework for challenging laws, systems, and regulatory structures that outsource enforcement to private, unaccountable actors. It is especially urgent in jurisdictions where constitutional protections are being circumvented through digital proxies and privatized compliance models.

This framework applies directly to legislation such as:

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

- **U.S. state-level age-verification laws** like Louisiana HB 142, which mandate identity checks for accessing constitutionally protected content but delegate the enforcement of those laws to private tech vendors without state oversight, appeals mechanisms, or public process.
- **Social media laws in Texas[38], Florida, and Utah[39]**, which require platforms to implement speech-related compliance rules in response to political pressure, effectively transforming private content moderation into state-mandated censorship, without acknowledging it as such.
- **Biometric identity systems across the EU, U.S., and Australia**, in which access to education, healthcare, or government services is conditioned upon facial scans or fingerprint data handled entirely by third-party platforms with little or no public scrutiny.
- **Educational technology mandates** that require students, especially minors, to participate in surveillance-based digital platforms as a condition of receiving state-provided education, without meaningful alternatives, opt-outs, or data protection guarantees.
- **International pandemic-era infrastructure**, including mobile health passports and geolocation check-ins that became de facto gatekeepers for mobility and participation in civic life, yet were operated by private companies under emergency contracts, often with no clear sunset clause or remedy for exclusion.

This doctrine can also be used to challenge the **structural features** of enforcement schemes:

- Cloud-based access systems where eligibility decisions are made by proprietary algorithms;
- Terms of service that function as law, with penalties for non-compliance but no legal review;
- Predictive enforcement tools used by police, immigration agencies, or welfare offices that automate penalties or trigger investigations without human intervention.

Across all of these domains, the legal theory provides a unified standard: **when a sovereign government requires its citizens to comply with a law, it must also own the enforcement[40].** It cannot shift the burden to private infrastructure, disclaim responsibility, and still claim to uphold constitutional values[41].

The doctrine is applicable to **litigation, legislative reform, regulatory review, and international advocacy**. It offers courts a standard for determining when enforcement has been unlawfully delegated. It gives litigants a cause of action grounded in constitutional and tort principles. And it provides policymakers with a red line: no matter how digital our systems become, the duty to enforce the law **cannot be outsourced without consequence.**

IX. Closing Statement

Sovereignty is not symbolic. It is the lawful power to govern, and the corresponding duty to do so transparently, accountably, and within the bounds of constitutional and human rights. When

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

sovereign governments outsource enforcement to private digital actors, they do not merely modernize. They **abdicate**.

This doctrine is a line in the sand. *Negligent Delegation of Digital Enforcement by Sovereign Governments*™ asserts that enforcement must remain in the hands of the public, even in the digital age. The right to access services, speak freely, move through public space, and participate in civic life cannot be gated by platform policies or commercial algorithms. Enforcement by interface is still enforcement, and if the state mandates it, the state must stand behind it[42].

The digital state is still a state. It cannot govern through proxies while denying its role. As platforms, sensors, and biometric systems increasingly mediate our public rights, the courts must reassert a timeless principle: **only the sovereign may enforce the sovereign law[43]**. And when it does so negligently, by handing that power to actors beyond public reach, it must be held to account.

This doctrine is not reactive. It is protective. It does not reject technology; it rejects the **invisible inversion of legal authority** that occurs when enforcement is coded into systems no one voted for, governed by contracts no one can challenge, and administered by actors no court can compel.

We do not live under the rule of law if law is enforced by the private terms of an undisclosed vendor. We live under something else entirely, and this doctrine is how we name it, challenge it, and restore the public's rightful place at the center of legal power.

Citations and Attributes

APA (7th Edition):
Starr, K. (2025). *Negligent delegation of digital enforcement by sovereign governments™: A framework for global constitutional accountability in privatized enforcement systems*. KStarr Enterprises, LLC. https://www.katherinestarr.com/citations/sovereign-digital-enforcement-katherine-starr.pdf

MLA (9th Edition):
Starr, Katherine. *Negligent Delegation of Digital Enforcement by Sovereign Governments™: A Framework for Global Constitutional Accountability in Privatized Enforcement Systems*. KStarr Enterprises, LLC, 2025. www.katherinestarr.com/citations/sovereign-digital-enforcement-katherine-starr.pdf

Bluebook (Legal):
Katherine Starr, *Negligent Delegation of Digital Enforcement by Sovereign Governments™: A Framework for Global Constitutional Accountability in Privatized Enforcement Systems*, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/citations/sovereign-digital-enforcement-katherine-starr.pdf

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

[1] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 587–88 (1952)
[2] Peter L. Strauss, "The Place of Agencies in Government: Separation of Powers and the Fourth Branch," *Colum. L. Rev.*84, no. 3 (1984): 573, 579
[3] Katherine Starr, Negligent Digital Architecture: How Platform Design Codifies Harm, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/negligent-digital-architecture/.
[4] Katherine Starr, Negligent Digital Access: When Platform Design Enables Harm, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/negligent-digital-access/.
[5] Katherine Starr, Digital Maritime Doctrine™: A framework for Global Accountability, KStarr Enterprises, LLC (2025) Https://www.katherinestarr.com/digital-maritime-doctrine/.
[6] *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 163 (1803)
[7] International Covenant on Civil and Political Rights, art. 2(3), Dec. 16, 1966, 999 U.N.T.S. 171
[8] *A.L.A. Schechter Poultry Corp. v. United States*, 295 U.S. 495 (1935).
[9] *Goldberg v. Kelly*, 397 U.S. 254 (1970).
[10] Louisiana H.B. 142, 2023 Reg. Sess. (La. 2023)
[11] Amnesty International, *Stop the Scan: The Use of Facial Recognition Technology* (2021), https://www.amnesty.org/en/latest/research/2021/10/stop-the-scan-facial-recognition-technology/
[12] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* 103–05 (Oxford Univ. Press 2019)
[13] Human Rights Watch, *How Dare They Peep into My Private Life?* (May 25, 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/children-rights-violations-governments
[14] Shoshana Zuboff, *The Age of Surveillance Capitalism* 248–51 (PublicAffairs 2019)
[15] U.S. Department of Defense, "DoD Awards Joint Warfighting Cloud Capability (JWCC) Contracts," Dec. 7, 2022, https://www.defense.gov/News/Releases/Release/Article/3244683/dod-awards-joint-warfighting-cloud-capability-jwcc-contracts/
[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), Official Journal of the European Union, L 277, 27.10.2022, p. 1–102
[17] World Economic Forum, "Building Resilient Digital Health Infrastructure," 2021, https://www.weforum.org/reports/building-resilient-digital-health-infrastructure/
[18] Privacy International, "Smart Cities: Utopian Vision, Dystopian Reality," 2021, https://privacyinternational.org/report/4586/smart-cities-utopian-vision-dystopian-reality
[19] U.S. Department of Education, "Fact Sheet: Protecting Student Privacy While Using Online Educational Services," Feb. 2014, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/PPRA%20Online%20Ed%20Tech%20fact%20sheet.pdf
[20] *West v. Atkins*, 487 U.S. 42, 54–55 (1988)

[22] *Palsgraf v. Long Island R.R. Co.*, 162 N.E. 99, 100 (N.Y. 1928) (Cardozo, C.J.)
[23] Philip Alston, UN Special Rapporteur on Extreme Poverty and Human Rights, "Report on Digital Welfare States," A/74/493 (2019), https://www.undocs.org/A/74/493

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED

[24] Katherine Starr, Negligent Delegation of Digital Enforcement™: A Framework for Constitutional Accountability in Platform Governance, KStarr Enterprises, LLC (2025), https://www.katherinestarr.com/citations/Digital-Enforcement-Katherine-Starr.pdf
[25] Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928) (Cardozo, C.J.)
[26] https://www.law.cornell.edu/wex/nondelegation_doctrine
[27] A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935)
[28] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 163 (1803)
[29] Fifth Amendment- https://constitution.congress.gov/constitution/amendment-5/
[30] Fourteenth Amendment- https://constitution.congress.gov/constitution/amendment-14/
[31] Philip Alston, UN Special Rapporteur, Report on Digital Welfare States, A/74/493 (2019)
[32] Goldberg v. Kelly, 397 U.S. 254, 267–71 (1970)
[33] Brentwood Acad. v. Tennessee Secondary School Athletic Ass'n, 531 U.S. 288 (2001)
[34] West v. Atkins, 487 U.S. 42, 54–55 (1988)
[35] Brentwood Acad. v. Tennessee Secondary School Athletic Ass'n, 531 U.S. 288 (2001)
[36] UN Human Rights Council, "The Right to Privacy in the Digital Age," A/HRC/48/31 (2021)
[37] ICCPR, Article 2(3), 999 U.N.T.S. 171 (1966)
[38] Texas House Bill 20, 87th Leg., 2d Spec. Sess. (Tex. 2021)
[39] Utah S.B. 152 and H.B. 311, 2023 Gen. Sess. (Utah 2023)
[40] NetChoice, LLC v. Paxton, 49 F.4th 439 (5th Cir. 2022)
[41] 143 S. Ct. 1780 (2023)
[42] U.S. Supreme Court: Carter v. Carter Coal Co., 298 U.S. 238 (1936)
[43] Philip Hamburger, *Is Administrative Law Unlawful?* (2014)

© 2025 KATHERINE STARR | WWW.KATHERINESTARR.COM | ALL RIGHTS RESERVED