Preliminary Concept Paper

Rebooting Administrative Enforcement for the Information Economy

TTI REDESIGNING THE GOVERNANCE STACK
GEORGETOWN LAW

Preliminary Concept Paper

Rebooting Administrative Enforcement for the Information Economy

JULY 22, 2026

Julie E. Cohen
Nina-Simone Edwards
Meg Leta Jones
Paul Ohm

Co-Signers:[1]
William Boyd
Niva Elkin-Koren
Woodrow Hartzog
Jevan Hutson
James Fallows Tierney
David Gray Widder

---

1 The ideas in this concept paper were developed in part through workshops held with academics and regulators. Some of the attendees have decided, as well, to co-sign the paper. Although not every one of the co-signers agrees with every idea set forth below, each supports the proposals overall. In addition to the co-signers, we would like to thank Hilary Allen, Hannah Bloch-Wehba, Samuel Buell, Ryan Calo, Daniella DiPaola, Charles Duan, Mike Konczal, Christina Lee, Mols Sauter, Alicia Solow-Niederman, Daniel Wilf-Townsend, and Erie Meyer for their participation in the academic workshop and their constructive and generous feedback. We thank Britney Firmin for research assistance. This work was developed with the support of the Tech & Public Policy program at the McCourt School of Public Policy at Georgetown University, the Ford Foundation, and the Economic Security Project.

Executive Summary

This report is part of a broader initiative focused on reimagining the role of the administrative state in the governance of a digital, data-driven economy. It considers mechanisms and arrangements for strengthening the enforcement of public mandates as a means to deter harmful practices and business models.

Agencies face significant obstacles to effective enforcement. They lack the authority to see inside opaque, algorithmically driven systems and to impose penalties that deter. Enforcement tends to target the corporation alone, insulating individual actors from personal responsibility. Many laws are policed by lone agencies whose enforcement decisions are largely invisible to the public, which leaves prosecutorial discretion unchecked and creates a single point of failure.

In response, we offer principles for reinvigorated enforcement. Agencies need enhanced visibility, the ability to trace how specific choices lead to harmful systems and to build forensic proof. They must use design as a remedial lever, mandating changes to harmful products and services. Effective deterrence also requires personal responsibility for CEOs, managers, and investors who act as co-architects of unlawful business models, and accountable enforcement built on oversight and coordinated decentralization among multiple enforcers.

Next, we propose specific legal mechanisms to operationalize these principles. Laws should require companies to document how policy is translated into code, grant agencies express authority to order the redesign of harmful products and services, and create regularized pathways for charging responsible executives, managers, and investors. We also propose mechanisms that cabin prosecutorial discretion, making enforcement decisions more visible and guaranteeing that the most serious violations carry meaningful, non-negotiable consequences.

Finally, to help implement these recommendations, we would extend a board proposed in our prior reports so that it can produce trial-ready forensic evidence, and we would create a new bureau to help agencies craft and police redesign orders. We also recommend a certification regime for responsible managers, statutory changes and deconfliction mechanisms to support coordinated enforcement across federal and state agencies, and a new office to monitor the enforcers themselves.

Introduction

Federal agencies lack the resources and legal authorities required to adequately police the information economy. Agencies lack the visibility they need into how regulated entities operate, which undermines their ability to detect harm and enforce public mandates involving opaque, algorithmically driven systems. They lack the authority and, sometimes, the will to impose significant penalties for corporate wrongdoing, and they lack both the express authority and the skill sets needed to mandate and supervise meaningful redesign of information-economy services. Enforcement most frequently targets the corporation alone, which diffuses responsibility and insulates executives, actively involved investors, and key managers from personal liability.

These challenges result in a system that comprehensively fails to address the harms caused by information economy actors. Typically, the system produces consent decrees that prioritize bureaucratic compliance systems over substantive changes, allowing firms to commission expensive audits while continuing to ignore the root causes of the harms they generate. Companies are incentivized to treat enforcement actions as manageable costs of doing business rather than as significant deterrents to harmful practices and business models.

To bridge this gap, it is necessary to adopt a strategy of direct deterrence that targets the two root causes of illegal behavior: the design of the systems and the choices of the individuals who profit from them. Effective enforcement must treat design as a regulatory lever, empowering enforcers to mandate specific changes to a company's internal structure and the design of its products and services. Additionally, effective enforcement must target the CEOs, middle managers, and even investors who act with knowledge of–or indifference to–the harms they cause.

In addition, we must shift the incentives of enforcers themselves. We propose moving beyond the "single cop on the beat" model, which creates a single point of failure, to a model based on productive competition among multiple agencies.[2] Our proposal attempts to offset the inefficiencies of redundancy with measures designed to encourage coordinated decentralization.

Part 1 identifies the structural obstacles to effective enforcement, which range from inability to monitor algorithmic systems to the diffusion of responsibility for organizational wrongdoing. Part 2 provides principles for reinvigorated enforcement, arguing for forensic visibility, a turn to redesign remedies, regularized pathways for individual accountability, and enforcement accountability through oversight and coordinated competition. Part 3 proposes specific legal mechanisms to operationalize these goals, including authority to order the redesign of defective products and services and authority to investigate and name responsible individuals. Finally, Part 4 details the institutional arrangements necessary to support these mechanisms, including specific measures to increase the number of enforcers and improve oversight of and coordination among them.

2 We are not focusing on the role of private enforcement in the form of lawsuits filed by plaintiffs' class action firms and civil society organizations. Much can be said about the role private enforcement might play to help shore up gaps in public enforcement. In this report, as in our other reports, we are focused on public agencies..

Part 1: Obstacles to Effective Enforcement of Public Mandates

Agencies face many significant and longstanding obstacles to effective enforcement.

As an overarching and threshold matter, Congress does not appropriate the resources that civil law enforcement agencies require to adequately police information-economy industries. Agency heads from both political parties routinely complain in annual testimony about their lack of resources. Lacking sufficient resources, agency staff cannot enforce at adequate levels. They therefore feel pressure to settle cases rather than engage in protracted litigation and, when contemplating litigation, to avoid complex cases. Resource constraints make all the obstacles identified below worse, and they are the most straightforward way to make progress on all of these fronts at once. No progress can be made without increasing support for civil law enforcement.

The problem of underinvestment has more recently been eclipsed by executive branch hostility to some of the most important civil enforcement agencies, most notably the Consumer Financial Protection Bureau (CFPB), which has been essentially dismantled by the second Trump administration. Rebuilding the CFPB and reinvigorating other affected agencies are prerequisites to the proposals we offer in this report.

However, resource constraints and politically motivated sabotage are only parts of the problem. Structural deficiencies prevent agencies from understanding and acting to deter many practices and business models that create serious and widespread harms.

Insufficient Investigative Authority

As described in our earlier concept paper on "Regulatory Monitoring in the Information Economy," federal administrative agencies largely lack the authority necessary to monitor the design, operation, and effects of digital systems and architectures.[3] Agencies and auditors also are not explicitly empowered to compel production of the technical, organizational, and operational data they need to have when they are investigating opaque, algorithmically-driven systems. As a result, agencies often develop incomplete or outdated views of how regulated entities operate, undermining their ability to detect harms and enforce existing mandates.

Our prior concept paper framed this lack of vision as an epistemic gap. Agencies (and by proxy, all of us) are fundamentally unable to know what is happening inside the companies that they are charged with regulating. Here, we emphasize that the epistemic gap is also an evidentiary shortfall: agencies cannot develop the kind of reliable and authenticated information they need to prevail in a civil trial (or, more realistically, to appear able to prevail in a civil trial, in order to extract a meaningful settlement.)

Inadequate Remedial Authorities

Congress also has not authorized enforcement agencies to impose the kinds of penalties that would serve as sufficient deterrents to illegal activities.

3 Julie Cohen, et al., Regulatory Monitoring in the Information Economy (2024), https://www.law.georgetown.edu/tech-institute/wp-content/uploads/ sites/42/2024/09/Regulatory-Monitoring-in-the-Information-Economy.pdf.

The ability to seek and recover meaningful financial penalties is one necessary component of effective deterrence. Without express authority to impose fines calibrated to the scale of the wrongdoing, agencies cannot ensure that lawbreakers confront a meaningful price tag. In particular, many commentators have noted that the Federal Trade Commission's (FTC) inability to fine firms that commit unfair and deceptive conduct in the first instance significantly limits its power.[4] Without the authority to seek equitable monetary penalties, agencies cannot disgorge ill-gotten gains or make victims whole. The FTC's powers have been weakened still further by a recent Supreme Court decision that found that the agency lacked the power to seek equitable restitution, and other agencies also have faced challenges to their disgorgement authority.[5]

Agencies also tend to underutilize their power to use injunctive relief to order the redesign of harmful products and services. This may be the result of a sense that government officials do not have the expertise to prescribe the fine details of industrial reconfiguration. Or it may stem from a fear that specific interventions risk judicial rejection or political rebuke. Regardless of the motivation, agencies tend to tinker around the edges of companies and their pathologies, seeking new structures for generalized compliance, such as "comprehensive" privacy or data security programs, or minor reconfigurations of organizational structure, such as board privacy committees or chief privacy officers.

To no surprise, companies subject to minor fines and symbolic injunctions are not deterred from breaking the law again, and their competitors are emboldened to follow their example.

Difficulty Operationalizing Remedial Orders

Many agencies have long prioritized settlement over litigation, and in settlement, most cases result in weak consent decrees that do not meaningfully alter corporate behavior.

For example, the FTC's consent decrees have proven to be incapable of discouraging subsequent violations. Typically, these decrees obligate the violator to implement a comprehensive privacy or data security program that prioritizes internal systems for monitoring rather than meaningful changes to consumer-facing products and services. Companies under consent decrees, a club that by this point includes most significant information-economy platforms and many other actors, can point to the staff positions they have created and the expensive audits they have commissioned. When subsequent violations occur, the FTC most often assesses a relatively small fine (with a few notable exceptions involving fines against Facebook and Amazon in the billions of dollars[6]) and enters into a new consent decree along the same lines.

By contrast, at least under the prior administration, the CFPB began to use consent decrees to impose harsher and more operationally specific remedies tied to the violations under investigation. For example, the CFPB prevented Goldman Sachs from launching new consumer credit card products after it launched the Apple Card with insufficient consumer protections.[7] Settlements like these, moreover, still do not compare to what a more complete remedial system could achieve.

---

4 *See, e.g.*, Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority*, 170 U. Pa. L. Rev. 71 (2021); David C. Vladeck, *The Erosion of Equity and the Attack on the FTC's Redress Authority*, 82 Mont. L. Rev. 159, 178-79 & n.151 (2021); Kurt Walters, *Reassessing the Mythology of Magnuson-Moss: A Call to Revive Section 18 Rulemaking at the FTC*, 16 Harv. L. & Pol'y Rev. 519, 525 (2022).

5 *AMG Capital Management v. FTC*, 593 U.S. 67, 76-77 (2021).

6 Press Release, FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook; Press Release, FTC, FTC Secures Historic $2.5 Billion Settlement Against Amazon (Sept. 25, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon.

7 *Goldman Sachs Bank USA*, CFPB, https://www.consumerfinance.gov/enforcement/actions/goldman-sachs-bank-usa/.

Another common practice that blunts the deterrent effect of settlements and consent decrees is the long-standing practice of allowing companies to "neither admit nor deny" (NAND) the allegations of wrongdoing. Much of the commentary–most of it critical–about this practice has focused on the Securities and Exchange Commission, which permits NAND provisions by rule.[8] Most notably, in a Southern District of New York opinion refusing to approve a settlement between the agency and Citigroup, Judge Rakoff criticized the practice for, among other things, permitting a company to treat settlement as a mere "cost of doing business" given the modest penalties involved.[9]

By liberating companies from obligations to change their behavior or even admit any wrongdoing, agency settlement practices blunt the deterrent effect of enforcement both for the targeted company and other companies. Companies considering a harmful or illegal action understand that in the unlikely event they are investigated and charged, the downside risks are low.

Lack of Personal Responsibility

Most enforcement cases against information economy actors result in liability for the corporation alone. Although agencies have the power to charge individual executives, they have done so only rarely. The result is less deterrence. Industry executives never fear being held accountable for the harms that result directly from their personal actions. Only the corporation's coffers are exposed–and, as the previous section explained, that exposure is minimal.

Freed from most external enforcement pressure, the high-ranking executives of many important information technology companies also feel little internal pressure to comply with the law because their corporate governance structure has been designed to avoid CEO accountability. Many such companies adopt a dual-class stock structure that gives founders (and in many cases, a sole founder) continuing voting control even when they retain less than 50 percent equity ownership. This arrangement removes pressure to account to shareholders and also reduces the authority of the board of directors (which may be stocked with members of the founders' inner circle).

Although executives have been charged in rare cases, lower-ranking managers are almost never charged. This is despite the fact that middle managers often bear direct responsibility for harmful decisions. Many insider accounts have documented how managers have refused to order changes to products and services that they knew were causing harm to vulnerable victims.[10] Even when unethical and exploitative business plans originate in the C-suite, it is middle managers who translate the plans into actionable form. Some companies devolve an unusual amount of power and responsibility to small teams. In other cases, platform harms originate with

---

8 17 C.F.R. § 202.5(e) (2010). *See, e.g.*, Verity Winship & Jennifer K. Robbennolt, *Admissions of Guilt in Civil Enforcement*, 102 Minn. L. Rev. 1077 (2018).

9 *SEC v. Citigroup Global Markets*, 827 F. Supp. 2d 328 (S.D.N.Y. 2011), *stayed pending appeal* 673 F.3d 158 (2d Cir. 2012). More recently, the SEC under the Trump administration rescinded an older rule that required settling defendants not to deny the allegations. Rescission of Policy Regarding Denials in Settlements of Enforcement Actions, 91 Fed. Reg. 29892 (May 21, 2026).

10 Insider accounts, including the Facebook Papers, have exposed how internal researchers and product teams at Facebook identified harms, yet proposed changes were delayed or rejected by decision-makers within the company. See Steven Levy, *Facebook Failed the People Who Tried to Improve It*, WIRED (Oct. 25, 2021), https://www.wired.com/story/facebook-papers-badge-posts-former-employees. Leaked internal documents from Uber reveal that instead of addressing harms, employees coordinated messaging strategies that leveraged violence against drivers for political influence, and at other times, reframed or downplayed known safety risks. *Uber Files: Uber broke laws, duped police and secretly lobbied governments, leak reveals*, The Guardian (July 10, 2022), https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign; *About the Uber Files Investigation*, Washington Post (July 11, 2022), https://washingtonpost.com/business/2022/uber-files-investigation/?itid=lb_read-the-investigation-the-uber-files_1.

vague goals (e.g., "increase engagement by 10%"), and it is middle managers who turn those goals into specific, harmful, design choices. Middle managers who feel a credible risk of personal accountability might act more often to push back, defy, or blow the whistle on illegal activity.

Finally, venture capitalists and angel investors demand extraordinary returns, some of which are captured by avoiding the expenses associated with legal compliance, yet these investors are never investigated much less charged by law enforcement agencies. Many information-economy businesses receive specific guidance from their funders. In some cases, venture capitalists, angel investors, and incubators and accelerators behave like system architects rather than mere funders. They don't just write checks; they demand specific business models and decisions that encourage excessive risk taking in pursuit of explosive growth.[11] They fund companies they know cannot operate legally, hoping that a "forgiveness rather than permission" approach will lead to popular pressure to change the law.[12] And they actively work to structure companies to insulate founders from the moderating influence that independent board members or major shareholders might exercise.

Unchecked Prosecutorial Discretion

In a world of limited resources, prosecutorial discretion is unavoidable. We simply cannot give enforcement agencies all they would need to investigate and prosecute every alleged violation of every law. In the right hands, prosecutorial discretion can be exercised as a tool of flexibility and justice. Agencies can align their enforcement priorities with the broader goals of their enabling legislation, the incumbent administration, and public sentiment, and they can pursue cases with the most deterrent impact. Unfortunately, prosecutorial discretion can also be employed in ways that cut against the public interest. It can be used to make important or meritorious cases languish or quietly disappear and mask the fact that an agency has been captured. Even agencies acting in good faith may prioritize quick symbolic wins over the hard slog of more meaningful enforcement.

The "single cop on the beat" model–in which single federal agencies hold exclusive or near-exclusive jurisdiction over particular sectors, issues, or categories of harm–compounds the downsides of unchecked prosecutorial discretion. Such agencies effectively dictate the entire enforcement landscape. A single decision not to press the law aggressively can unilaterally undercut the effectiveness of a public mandate or functionally immunize certain lawbreakers.

Lack of visibility into enforcement decisions contributes to the risk of systemic underenforcement. Such decisions are treated as highly confidential for good reasons: to protect strategic advantage and to prevent public prejudgment of guilt. But the necessary cloak of confidentiality means that enforcers have no fear of being second-guessed when they abandon their mandates or succumb to industry capture.

Finally, even when an agency decides to bring charges, unchecked prosecutorial discretion allows it to settle cases too quickly and too leniently. With no lower limits on the nature or severity of remedies they may impose in settlement, agencies too often negotiate away their leverage.

---

11 Tim Sullivan, *Blitzscaling*, Harv. Bus. Rev. (Apr. 2016), https://hbr.org/2016/04/blitzscaling; Brian J. Broughman & Matthew T. Wansley, *Risk-Seeking Governance*, 76 Vand. L. Rev. 1299, 1342 (2023).

12 Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. Cal. L. Rev. 383 (2017).

Part 2: Principles for Reinvigorated Enforcement

Our central goal is to equip agencies to demand and incentivize compliance with the law, thereby reducing harms to individuals, groups, and the public at large. Therefore, although we believe there is a role to be played for other enforcement goals, such as restitution, retribution, and rehabilitation, we are focused on the goal of deterrence, in both its specific and general forms. Currently, it is rational for companies and their executives to bet that they will never fall under enforcement scrutiny. Such bets yield material advantages: access to markets that others fear breaking the law to enter (Uber), valuable data that others refuse to collect or process (Facebook), or decreased compliance costs compared to those that more law-abiding companies have to bear. We seek to change that calculus.

We motivate and organize the mechanisms in Part 3 and the administrative reforms in Part 4 with four overarching principles: First, agencies need the tools to establish forensic proof of wrongdoing. Second, they need authority to mandate remedial redesign of products and services. Third, personal responsibility is an essential component of effective deterrence. Finally, effective enforcement requires a resilient prosecutorial ecosystem that balances coordination and competition.

Forensic Visibility

Enforcement cases are built on evidence, so it is vital to ensure that enforcement agencies have adequate investigative tools. Understanding the behaviors of digital systems in practice depends on understanding the organizational decisions, workflows, and dynamics that shape them. Our prior concept paper on "Regulatory Monitoring in the Information Economy" identified mechanisms for increasing visibility into how organizations function internally. As we shift to enforcement, these tools of visibility become useful for establishing forensic proof, which demands a granular, unbroken chain of evidence that can withstand adversarial and judicial scrutiny.

A central goal for enforcement should be to trace the exact workflow of decisions. To prove liability, enforcers must understand that digital systems and services are the summed action of specific human choices. Forensic proof requires isolating those choices–and identifying the specific individuals (from the CEO to the middle managers) who had the authority, foresight of harm, and power to intervene. Special attention should be paid to engineering choices. Enforcers should trace how high-level business priorities are formally translated through internal directives, training materials, and routine practices into architecture, algorithms, and interfaces.

Finally, forensic proof requires looking beyond formal job titles to unearth deeper chains of accountability. Coercion and control may originate outside the traditional corporate hierarchy. Enforcers need to be able to map the structural and financial pressures, such as pressures from venture capitalists, that motivate illegal behavior.

Design as a Remedial Lever

Effective enforcement must encompass remedial redesign of organizations and their offerings. In the pre-digital age, this may have taken the form of negotiating changes to the structure and operation of a factory production line or a corporate R&D program. For companies that offer networked digital systems, many have written about the importance of treating *design* as a regulatory

lever.[13] We have written about this principle before, in our report on "Designing Policymaking Mechanisms for Regulatory Dynamism." There we described some of the design goals regulators might seek, such as injecting seams and friction into services designed to be seamless and frictionless. We also proposed a system by which agencies could issue *ex ante* design specifications that certain companies would be obligated to follow.

Enforcers play an important role in seeking the redesign of products and services to eliminate the root causes of certain important harms. The principle of remedial redesign should be applied across all layers of a platform's technology stack. At the user-interface level, for example, enforcers should seek to remove specific design features that make products manipulative (e.g. dark patterns) or addictive (e.g. infinite scroll). At the backend infrastructure level, enforcers can insist on hardware-level data isolation to create a verifiable governance seam–a discontinuity or other deliberately created point injected into systems to make them more legible and more amenable to governance.[14] For example, when a company acquires a massive trove of sensitive user data during a merger, enforcers might require segmenting the sensitive information into a separate dataset rather than merging it in with other data. Finally, at the algorithmic level, enforcers might turn to algorithmic disgorgement–the mandatory deletion of the model itself–or to mandatory modifications to algorithmic design parameters.[15]

Personal Responsibility

As noted above, digital systems and services are the summed results of specific human choices; effective deterrence should aim to produce different specific choices. Enforcers therefore should consider the responsibility of a broad range of individual decisionmakers, not only the companies that employ them.

First, when the CEO and the firm are functionally indistinguishable due to the way they have structured the corporate form, enforcement must target the individual holding the absolute control. Second, enforcers should ascertain whether harms result from decisions by mid-level managers such as program directors and lead engineers. To be clear, we don't recommend targeting junior developers who make innocent mistakes or middle managers whose efforts to keep the firm on the right side of the law are overruled by others higher up the chain of authority. We do recommend charging responsible parties who act with foresight of the harms they are causing. Finally, law enforcement tools should allow agencies to investigate and charge funders who are also co-architects of unlawful business practices.

Accountable Enforcement

Constructing a more robust and effective enforcement ecosystem requires meaningful oversight of the enforcers themselves. To accomplish this, we envision a shift from the "single cop on the beat" model described above to a distributed enforcement network, guided by three subprinciples: oversight, mandatory baselines, and structured coordination.

To ensure that enforcement decisions align with public mandates rather than hidden concessions, the exercise of prosecutorial discretion must be visible and legible to both the public and other regulatory actors. The challenge involves increasing transparency without compromising the important benefits of investigative confidentiality. In Parts 3 and 4, we propose mechanisms for doing just that, including new reporting obligations and independent oversight institutions designed to identify and disrupt systematic patterns of underenforcement or political interference.

---

13 *See, e.g.*, Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018).

14 Brett Frischmann & Paul Ohm, *Governance Seams*, 36 Harv. J. L. & Tech. 1117 (2024).

15 Final Order at 4, *In re* Cambridge Analytica, LLC, No. 9383 (FTC Nov. 25, 2019) (ordering Cambridge Analytica to "[d]elete or destroy all Covered Information collected from consumers through GSRApp, and any information or work product, including any algorithms or equations, that originated, in whole or in part, from this Covered Information.").

The enforcement system must guarantee minimum, non-negotiable consequences for the most egregious or repetitive harms, ensuring that the worst offenses cannot too easily be settled away. The goal is to transform enforcement penalties from manageable costs of doing business into genuine deterrents that compel meaningful changes in corporate behavior. In Part 3, we propose mechanisms designed to replace episodic enforcement with systematic scrutiny.

In the civil enforcement context, we think a single point of failure has prevented effective enforcement too often. The challenge involves avoiding wasteful redundancy or counterproductive turf wars.[16] Our goal is *coordinated decentralization*, accepting some inefficiencies of overlapping jurisdiction to gain efficacy and resilience against capture.

If the right balance can be struck, both cooperation and competition produce important benefits. In cooperative enforcement environments, agencies can marshal a diverse set of resources, expert specialization, statutory authorities, and procedural tools, thereby strengthening overall enforcement capacity. In recent years, many high-profile investigations and lawsuits have been brought by large coalitions of state AGs and federal agencies working together, often with one federal agency or state attorney general acting as the lead.[17] This allows smaller agencies and states to leverage resources and expertise that they could not use on their own. In our deeply divided country, coordination can also help bridge political divides, as witnessed in the myriad cases in which blue state and red state AGs have joined forces to sue a tech giant for antitrust or consumer protection violations.

Turning from the benefits of coordination to the strengths of competition, agencies often gain reputational benefits through specialization. We see evidence of this in Illinois and Texas, which have used their unusually aggressive facial recognition laws to bring national attention to their enforcement work against the largest tech firms.[18] Another example of a healthy rivalry is the European Union, whose data protection authorities often jockey to be the lead agency investigating a high profile company accused of novel violations of the GDPR.[19] Parallel enforcement designed right can also mitigate the harms that result from the capture of any single agency. In Part 4, we propose several mechanisms to increase positive regulator competition.

---

16 A substantial (though not unanimous) body of administrative law scholarship recognizes that conflict and competition among agencies are routine and often productive features of the administrative state. See Daniel A. Farber & Anne Joseph O'Connell, *Agencies as Adversaries*, 105 Cal. L. Rev. 1375 (2017); Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space,* 125 Harv. L. Rev. 1131 (2012) (describing routine agency coordination); Max J. Minzner, *Should Agencies Enforce?*, 99 Minn. L. Rev. 2069 (2015) (noting horizontal competition for financial incentives). *But see* Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, 98 Cornell L. Rev. 769, 803 (2013) (arguing that "centralization may be more efficient . . . centralized control ensures consistency . . . [and] . . . increases accountability").

17 Press Release, U.S. Department of Justice, Justice Department Sues Google for Monopolizing Digital Advertising Technologies (Jan. 24, 2023), https://www.justice.gov/archives/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies; Press Release, Office of the Maine Attorney General, Attorney General Aaron M. Frey Announces Multistate Lawsuit against Meta for Social Media Harms to Children (Oct. 24, 2023), https://www.maine.gov/ag/news/article.shtml?id=12023754#:~:text=The%20lawsuit%20alleges%20that%20Meta:%20*%20Designed,rectify%20the%20harms%20caused%20by%20these%20platforms; Press Release, Montana Department of Justice, Attorney General Knudsen launches investigation into big tech companies (Sept. 24, 2025), https://dojmt.gov/attorney-general-knudsen-launches-investigation-into-big-tech-companies/.

18 *See, e.g.*, Alfred Ng, *Meta agrees to pay Texas $1.4 billion in largest state data privacy settlement*, Politico (July 30, 2024), https://www.politico.com/news/2024/07/30/meta-texas-settlement-00171823.

19 *Data Protection Commission loses EU court challenge to EDPB's authority*, Irish Legal News (Jan. 29, 2025), https://www.irishlegal.com/articles/data-protection-commission-defeated-in-eu-court-challenge-to-edpbs-authority?; *Economic & Reputational Risk of the DPC's Failure to Uphold EU Data Rights*, Irish Council for Civil Liberties (April 9, 2021), https://www.iccl.ie/digital-data/economic-reputational-risk-of-the-dpcs-failure-to-uphold-eu-data-rights/; *see also* Elvira Pollina & Alvise Armellini, *Italy fines OpenAI over ChatGPT privacy rules breach*, Reuters (Dec. 20, 2024), https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/.

Part 3: Mechanisms for Operationalizing Effective Enforcement

To translate the principles outlined in Part 2 into reality, agencies require a new suite of legal authorities empowering them to move from broad oversight to decisive action. This Part offers four sets of specific measures to operationalize this shift. First, agencies should have the evidence toolkit needed to identify and successfully prosecute violations. Second, we call for explicit remedial redesign powers, which agencies can invoke to mandate changes to harmful products and services. Third, we introduce mechanisms to establish personal accountability, including "accountability autopsies" and express authority to investigate and charge executives and "strategic architect" investors. Finally, we offer several mechanisms for cabining and channeling prosecutorial discretion, including declination reports, permanent enforcement dockets, and mandatory penalty triggers.

Mandatory Diff Mapping

Congress must grant agencies the authorities they need to pivot from the "audit toolkit" described in our concept paper on "Regulatory Monitoring in the Information Economy" to the "evidence toolkit" required at enforcement. Our prior concept paper discussed the importance of access to internal policies and training materials that might shed light on a company's priorities. Enforcers will care as well about whether and how those priorities were then translated into code. More specifically, they will want to understand the "diff" (to use the geek's term) between what the policies say and the engineers implemented.[20]

Congress should impose a statutory duty on all except the smallest information-economy actors to track and document how policy becomes code inside their organizations by creating what we will call "diff maps." The path between managerial directive and running code can vary wildly based on institutional practices, cultures, and internal controls. For example, an executive mandate to "seek user consent to process precise geolocation information," perhaps because a new state comprehensive data privacy law requires it, triggers a complex chain of translation from natural language into source code. Tracking the diff forces a company to map the exact workflow: Which departments or working groups are involved? Which workers inside those departments possess what kind of training? How do imprecise terms such as "consent" and "precise" get translated? Are these decisions enacted top-down by counsel or bottom-up by engineers?

Diff maps should document not only the intentional choices of individuals and teams but also the emergent and multifaceted behaviors that arise in complex, algorithmically driven organizations and systems. For example, if management sets aggressive advertising sales targets, engineers might tune their services to spur greater addictive engagement or more invasive user surveillance. Or a reinforcement learning system configured to maximize stock trading returns might lead to unintended fraudulent or illegal conduct such as front running or pump-and-dump schemes. A successful diff map will trace these incentives and mechanisms. Each covered company will need to generate diff maps any time its internal operations shift.

20 In UNIX-like systems, the diff program lists all differences between two files (typically two versions of the same source code file at different moments in time) in a compact output format. *GNU Diffutils Manual*, GNU Operating System (version 3.12, Jan.12, 2025), https://www.gnu.org/software/diffutils/manual/html_node/index.html. Geeks now use the word generally to describe assessments of the difference between two data sources or systems.

Diff maps are closely related to–and build upon–the "accountability graphs" we called for in "Regulatory Monitoring in the Information Economy." We described those as better org charts that map not only titles and reporting relationships but also the workflows within a company. Diff maps are accountability graphs augmented with greater technical detail. Most companies will build their accountability graphs and diff maps at the same time.

The obligation to create diff maps will give companies an incentive to pay closer attention to how their policies are implemented, and the process of creating the maps will help some of them notice inconsistencies before they turn into problems. And when problems do arise, enforcers will be able to obtain diff maps as key inputs into their investigations, for example to help in the preparation of the accountability autopsies discussed below.

Preparing accurate diff maps will often prove to be complicated and expensive, and some companies might be tempted to treat this obligation as a check-the-box compliance exercise. To discourage this, agencies should be empowered to cite incomplete or inaccurate diff maps as themselves violations of law. They should assess the rigor and care with which a company's diff maps have been created, not only during investigations but in connection with other regulatory monitoring obligations imposed by statute or consent decree, such as mandatory audits and on-site inspections.

Explicit Remedial Redesign Authority

Congress should clarify that all agencies with jurisdiction over information economy actors have the remedial power to require the redesign of products and services.

We have earlier proposed an *ex ante* public role in specifying standards for the design of safe products and services. In our concept paper on "Designing Policymaking Mechanisms for Regulatory Dynamism," we proposed that agencies with regulatory authority over information economy actors "should be empowered to establish and mandate adherence to clear specifications for the design of digital interfaces from the outset."

Any such *ex ante* design authority must be backed by robust enforcement powers. Agencies must be given the power and tools they need to detect, investigate, charge, litigate, and settle matters involving noncompliance with their design specifications. Crucially, they must be given the express power to seek injunctions ordering the redesign of products and services.

Even in the absence of *ex ante* design specifications, agencies should have the express power to seek appropriate redesign remedies for violations of the law. Agencies that have been given the broad authority to seek injunctions, such as the FTC, arguably have such power now, but there is scant authority for this.[21] Other agencies have more specific authority that relates to redesign. For example, CFPB can order "rescission or reformation of contracts."[22] Since many financial services are defined by their contracts, when the CFPB orders reformation of contracts, it has effectively forced the company to redesign the offering. The FCC has the express power to recall some radio-frequency hardware, but this has been narrowly interpreted.[23] Congress should foreclose any

21 15 U.S.C. § 53(b). Note that in *AMG Capital Management v. FTC*, 593 U.S. 67 (2021), the Supreme Court read this provision narrowly, holding that the FTC lacked the ability under it to seek restitution or disgorgement of profits.

22 12 U.S.C. § 5565(a)(2).

23 47 C.F.R. § 2.939 (2025) ("Revocation, withdrawal, or limitation of equipment authorization").

doubt about the scope of remedial redesign authority by granting all agencies charged with overseeing information economy actors the express power to seek the redesign of organizations and their offerings to remove or limit their harm-causing features.[24]

One model for the kind of redesign authority we envision comes from laws that protect consumers from defects in mass-produced products. For example, the Consumer Product Safety Act (CPSA),[25] the National Traffic and Motor Vehicle Safety Act,[26] and the Federal Food, Drug, and Cosmetic Act,[27] give the Consumer Product Safety Commission (CPSC), National Highway Traffic Safety Administration (NHTSA) and Food and Drug Administration (FDA), respectively, recall or recall-like powers over defective products. In the case of the CPSC and FDA, this power is referred to as the power to order "repair, replacement, or refunds".[28] The NHTSA law refers to this as the power to order the manufacturer to "remedy the defect."[29] A recall-like approach would give the company the initial opportunity to decide for itself whether to remedy the product or service through repair, replacement, or refund but grant the agency the power to reject the redesign proposal.[30] If the company cannot propose an alternative plan that meets the agency's approval, the agency should have the power to remove the product or service from the market.[31]

Regularized Pathways for Charging Individual Actors

Enforcers need new mechanisms that allow them to hold individuals responsible for their roles in conceptualizing, planning, and implementing corporate wrongdoing. In Part 2, we identified three different categories of relevant actors: CEOs and other founders, middle managers acting with foresight, and financial backers. We propose mechanisms to make it easier to reach all three of these. We start with a tool for identifying the responsible parties: the accountability autopsy.

Accountability Autopsies

To help implement this statutory authority, in any investigation that leads to the filing of charges, the agency should be required to trace and document the full chain of responsibility for all of the actions (or omissions) that led to the violation. They should document what they learn in an "accountability autopsy report" that lists every directly or indirectly responsible party and the circumstances that prevented them from avoiding or reporting the violation. The starting point for the accountability autopsy will be the company's most recent diff map, for those required to generate them. The company's account of how its policies were implemented in code will give the agency a company-defined road map of its own procedures for turning policy into code.

---

24 Indeed, this power was proposed by then-law professor Elizabeth Warren in an article credited as a key inspiration for the CFPB. Elizabeth Warren, *Unsafe at Any Rate*, Democracy Journal (Summer 2007), https://democracyjournal.org/magazine/5/unsafe-at-any-rate/ (calling for a "Financial Product Safety Commission" with redesign power modeled after the Consumer Products Safety Commission).

25 15 U.S.C. § 2064.

26 49 U.S.C. § 30118.

27 21 U.S.C. § 360h.

28 15 U.S.C. § 2064(d); 21 U.S.C. § 360h(b).

29 49 U.S.C. § 30118(b).

30 *Id.* at § 2064(d)(3)(B).

31 *Id.* at § 2064(d)(3)(C).

Preparing the accountability autopsy might require research through the historical record, tracing the actions of staff who have since departed and reconstructing org charts that look different than they do in the present day. In cases involving complex supply chains of developers, deployers, and customers, it also may require identifying responsible actors outside the targeted company. Armed with the accountability autopsy, agencies will be able to identify the exceptional cases when they should charge managers or line employees. When the autopsy points to companies and other responsible parties beyond the companies under investigation, it may lead to a recommendation to expand the investigation.

An accountability autopsy should be required even when a case leads to settlement and a consent decree. The time and effort required to compile the autopsy will diminish the incentive to cut the investigation short with a quick settlement. The completed autopsy will help the agency better appreciate the gravity of the activity, the likelihood of recidivism, and the best levers to pull in the settlement negotiations.

Executive Accountability Framework

For CEOs, other high-ranking executives, and founders, we propose codifying a new "executive accountability framework" either via a standalone statute or in the statutes establishing civil enforcement powers for the various agencies discussed in this concept paper. This framework modernizes the traditional "responsible corporate officer" doctrine developed in other areas of the law. In food and drug law, individual criminal liability attaches to an officer with the "responsibility and authority" to prevent or correct a public welfare violation, regardless of personal intent or awareness.[32] Over the years, the doctrine has been extended to issues of environmental safety,[33] financial governance,[34] securities regulation,[35] and state[36] and local[37] law. Provisions like these were developed to protect public health and safety, and that logic readily extends to the public health and safety threats caused by major technology platforms and other significant information economy actors.[38]

Under our proposed framework, executives in designated information-economy industry sectors would owe a statutory public-welfare obligation that supersedes traditional corporate shields, making them individually subject to strict liability for corporate misdeeds. The framework would extend to sectors determined by statute or rule with a track record of creating an unreasonable risk of certain harms (e.g. addiction, foreign interference in elections, or worker exploitation), such as companies offering social media, gig economy, or AI chatbot services. Executives at those designated companies would have a legal duty to actively monitor for and prevent those harms. They would no longer be able to use the excuse, "I didn't know about this" or "that decision was made by someone below me." In other words, it would impose on the executives both the obligation to investigate the effects of their products and services and the responsibility to address identified harms.

---

32 21 U.S.C. §§ 331 & 333; *United States v. Dotterweich*, 320 U.S. 277 (1943); *United States v. Park*, 421 U.S. 658 (1975).

33 Clean Water Act, 33 U.S.C. § 1319(c)(6); Clean Air Act, 42 U.S.C. § 7413(c)(6).

34 Sarbanes-Oxley Act, 15 U.S.C. § 7241.

35 15 U.S.C. § 78t(a).

36 California Corporate Criminal Liability Act, California Penal Code § 387.

37 N.Y.C. Admin. Code § 27-2004(a)(45) (defining a liable "owner" under the city's housing maintenance code to include any individual officer, firm, or corporation "directly or indirectly in control of a dwelling").

38 *See, e.g.*, Benjamin Zablotsky, et al., *Associations Between Screen Time Use and Health Outcomes Among US Teenagers,* 22 Preventing Chronic Disease 1 (2025); Office of the Surgeon General, Social Media and Youth Mental Health (2023); Emily Denniss & Rebecca Lindberg, *Social media and the spread of misinformation: infectious and a threat to public health*, 40 Health Promotion Int'l 1 (2025).

Agencies also should adopt enforcement policy statements stating the priority to investigate and prosecute individual executives for the laws that are broken under their watch. This should emphasize companies organized with dual-class stock arrangements and weak board authority that allow CEOs and other executives to operate with uncommon autonomy. For companies with these arrangements, the presumption should be that any enforcement action will be brought against the controlling executive. This presumption may be rebutted only after the investigation suggests the CEO lacked the shared responsibility for the specific harm, for example if a lower-level manager made the culpable decisions without informing upper management.

Non-Executive Employee Responsibility

Although it should not be as common nor as easy to establish liability for other employees, agencies need the power and discretion to charge managers and even frontline developers who act with foresight of the serious harms they caused. Congress should amend the laws that provide enforcement authority to the FTC, CFPB, FCC, and other information economy enforcement agencies to expressly grant them the authority to name individuals in their enforcement actions, to prevent any doubt. Individual liability should extend to those who knew that the design of a product or service posed a specific and severe risk of harm (based on internal data or warnings) and provided substantial direction or assistance to the team implementing the harmful feature.

We might mitigate the bite of this potential liability for managers by creating a safe harbor for meaningful and documented dissent. Borrowing inspiration from whistleblower protection laws and from the State Department's "dissent channel,"[39] the law could require companies to establish formal channels for logging dissent that are designed to apprise executives of concerns from the workforce.[40] During any investigation into possible individual liability, the presence of a timely and thorough dissent report filed in this channel can serve as a defense.

Strategic Architects

Finally, we propose a two-step approach for holding certain investors accountable for the violations they cause. First, Congress should create a new reporting obligation requiring companies to designate "Strategic Architect" investors to the SEC and to any agency with enforcement authority over the company's activities or product/service offerings, such as the FTC and/or CFPB. In these reports, companies would be required to name any investors who had imposed certain requirements of the kind that, in the past, have both contributed to lawbreaking and cut against the arguments for investor immunity. Possible examples include investors who insist on unremovable founder control or business models known to violate the law. The statute would direct the SEC, working in consultation with the agencies that expect to receive these reports, to enumerate the characteristics of investment terms, relationships, or structures that trigger the requirement. Since many of the relevant investment behaviors happen well before a company is taken public, the new reporting requirement would apply to pre-IPO offerings in addition to public company reporting.[41] And in case any early-stage investors have managed to avoid the obligation, the IPO filing itself can be a triggering event for identifying all of the Strategic Architects the firm has had, dating back to its founding.

Second, Congress should give agencies such as the FTC and CFPB the express power to charge designated Strategic Architect investors in cases linked to the misconduct they caused. One notable precedent for this enforcement

39 *2 Foreign Affairs Manual 070 ("Dissent Channel")*, U.S. Dep't of State, https://fam.state.gov/fam/02fam/02fam0070.html.

40 See Hannah Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, 118 Nw. U.L. Rev. 1503 (2024).

41 This might follow the approach of the "Bad Actor" rule from Dodd-Frank that disqualifies issuers from using the standard private-offering registration exemption if any investor has a prior criminal conviction (or regulatory sanction) relating to the purchase or sale of a security. 17 C.F.R. § 230.506(d).

approach is the action against Climb Credit filed in the waning days of the Chopra CFPB.[42] The agency sued student loan provider Climb for abusively and deceptively encouraging consumers to take loans based on false statements about the quality of certain educational programs. Notably, the agency sued (and quickly settled with) not only the company but also the investors who originally incubated Climb Credit under a provision permitting the CFPB to charge those who "provide substantial assistance" to a party that violates the law.[43]

Mandatory Enforcement Floors

We offer several new proposals designed both to limit prosecutorial discretion and to make prosecutorial choices more visible. To begin, Congress should end the standard practice of allowing companies to "neither admit nor deny" allegations in settlements. Removing this practice will subject companies to added deterrent pressure–including increased exposure to suit by their injured victims. Beyond this simple fix, we recommend three additional changes.

First, we propose a new law requiring enforcement agencies to issue "declination" reports in certain cases after concluding that an arguable violation of the law does not merit filing charges. Such notices must provide some detail about the steps taken in the investigation and the rationale for the decision not to enforce. Sharing this information will serve many purposes. Advocates and academics will be able to scrutinize the reports and raise flags about faulty reasoning or suspicious circumstances. Congress will gain better understanding of how laws are operating and may develop ideas for bolstering gaps. Other agencies with expertise and jurisdiction over the industry actor or the conduct under investigation can decide whether to bring a second investigation. And state officials can decide whether to step in where the federal government will not.

A "declination" report will not be appropriate after every closed investigation. A report announcing that a company was investigated for possible illegal activity may injure the firm's reputation even if the investigation has thoroughly absolved it of wrongdoing. Such reports should be triggered only for investigations that: have been publicly announced by the agency or otherwise credibly reported to the public; involve a company under enhanced regulatory scrutiny because it is subject to a consent decree or has been placed on a "permanent enforcement docket" (discussed below); or have resulted in the development of an extensive evidentiary record before the decision not to initiate formal proceedings.

Second, the most important information economy platforms are not episodic actors and should be subject to permanent enforcement dockets. One source of inspiration for this recommendation is the "Special 301" report process used by the U.S. Trade Representative.[44] That mechanism identifies foreign countries with inadequate intellectual property protection or other market access barriers for U.S. right holders. The process involves public comments and interagency investigation and concludes by listing countries on a "Priority Watch

42 *CFPB Takes Action Against Climb Credit and Investment Firm 1/0 for Deceiving Borrowers About Coding Bootcamps and Vocational Programs*, CFPB (Dec. 5, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-climb-credit-and-investment-firm-1-0-for-deceiving-borrowers-about-coding-bootcamps-and-vocational-programs/.

43 Complaint, Consumer Financial Protection Bureau v. Climb Credit, Inc. et al., No. 1:24-CV-07868 (S.D.N.Y. Oct., 17, 2024); 12 U.S.C. § 5536(a)(3) (specifying "substantial assistance" liability).

44 Special 301, U.S. Trade Rep., https://ustr.gov/issue-areas/intellectual-property/special-301; Sean Flynn, *What is Special 301? A Historical Primer*, InfoJustice (May 1, 2013), https://infojustice.org/archives/29465.

List" or "Watch List," which can trigger further trade actions. We envision that the FTC, the CFPB, and other relevant enforcement agencies could use a similar mechanism to scrutinize the actions of companies large enough or critical enough to qualify for a permanent enforcement relationship.[45]

Finally, for particularly egregious violations and for repeat offenders, we should mandate minimum, automatic sanctions. For example, Congress could amend the FTC Act to require minimum sanctions for certain violations of section 5 that: result in serious physical or emotional injury; target vulnerable people such as children, older adults, or people with disabilities; or represent repeat offenses. Penalties might be financial or might take the form of forced restrictions on a company's business activities, such as temporary bans from offering certain services.

---

45 In a separate concept paper, *Legitimacy and Accountability in the Information-Era Administrative State*, we propose a framework in which designated agencies are authorized to identify relevant indicators of harm or threats, monitor the indicators, and take preventative action. Under this model, multiple agencies would have enforcement powers to act on companies large and/or critical enough to qualify for a permanent docket.

Part 4: Institutional Arrangements for Ensuring Effective Enforcement

Operationalizing the new authorities we propose in Part 3 will require new institutional capacity. This Part outlines the necessary structural reforms to sustain this work. First, we would expand the capabilities of the Digital Architectures, Systems, and Processes Oversight Board (DASPOB) we proposed in our concept paper on "Regulatory Monitoring in the Information Economy." Second, we propose a "Digital Redesign Bureau" (DRB), a centralized resource that can assist agencies in crafting and policing product redesign orders. Third, we propose a mandatory system for certifying non-executive employees with significant, enumerated user-protection responsibilities. Finally, to manage the shift toward competitive enforcement, we propose new deconfliction mechanisms and the creation of an Office of Enforcement Accountability (OEA). This independent body will monitor the enforcers themselves, ensuring that prosecutorial discretion is not abused to let meritorious cases languish.

Building Forensic Capability

We would build on our earlier proposal for a Digital Architectures, Systems, and Processes Oversight Board (DASPOB) to ensure it produces the kind of actionable evidence needed in enforcement actions. We have already discussed examples of the different outputs the two phases require. The accountability autopsies generated during the evidence phase need to be more detailed than the diff maps and accountability graphs produced in the audit phase. For example, if a company's internal policies explicitly require the kind of guardrails that would have prevented a particular realized harm, and its diff maps suggest that those policies were faithfully translated into code, the autopsy might involve a detailed technical examination of whether the guardrails were properly implemented, and if not, precisely how they failed.

To support the production of these kinds of outputs, we would create two offices within the Board, charged with different standards of evidence production. The audit bureau would focus on increasing visibility and producing intelligence about specific industry actors and market-wide industry trends. The evidence bureau would focus on the kinds of information needed to successfully prosecute a case.

To support the principle of coordinated decentralization, staff charged with supporting forensic visibility should assist enforcers in developing a "common file" to be shared with agencies with overlapping authority, including state agencies. This file should be shared with any other federal or state agency with enforcement jurisdiction over the matter that requests it, barring a compelling reason to withhold it.

Supporting Remedial Redesign

We also propose a products-recall-style support structure for agencies that police the information economy. Most agencies will lack the personnel, experience, and monitoring capability to successfully implement this proposal. Although each agency that receives this charge will need to change its internal structure, we might develop some of the needed capabilities in a single agency, which we will call the Digital Redesign Bureau (DRB). The DRB would not have any enforcement power of its own. Instead, it would provide agencies such as the FTC, FCC, and CFPB with the expert advisors and tools to assist remedial redesign activities.

For example, the DRB would employ Human-Computer Interaction (HCI) and User Experience (UX) experts with experience designing large, complex, modern, and consumer-facing products and services. This corps would be consulted early in any investigation to help enforcers draft subpoenas that cover the information needed to develop redesign mandates. It would

also be involved during settlement negotiations to help the government's negotiators understand what redesign requests are feasible.

Enforcers can continue relying on the expertise of the DRB as they shape redesign remedies. During consent decree negotiations, for example, the DRB can vet the company's proposals for redesigning its products and services to help enforcers decide whether and how to make counterproposals.

Tracking Personal Accountability and Responsibility

Earlier in this concept paper, we proposed extending liability to certain employees who have both foreknowledge and the ability to intervene to prevent specific and serious harm. The Senior Managers and Certification Regime (SM&CR) created in the UK after the 2008 financial crisis offers a model for the sort of system we envision.[46] The SM&CR is designed to address cultural failures–i.e., organizational norms and incentive structures that normalize diffuse responsibility and profit over professional accountability–by clarifying where responsibility lies within firms.[47] It requires firms to issue "Statements of Responsibilities" (SoRs) for senior managers, which clearly state "what they are responsible and accountable for" and requires regulator approval before those managers can begin their roles.[48] Regulators have the power to hold the individuals who are subject to SoRs accountable after certain failures.[49]

Additionally, regulated firms must certify non-manager employees who are responsible for certain functions with "significant impact on customers and/or the firm."[50] For example, firms must certify staff who hold roles such as "proprietary trader," "significant management," "material risk takers," and "algorithmic trading."[51]

At the same time, the SM&CR's track record illustrates important design and enforcement challenges. Scholars have consistently noted low levels of enforcement against individuals, low financial penalties, and delays in enforcement.[52] Therefore, they have questioned whether the regime provides sufficient deterrence. There is ambiguity around what constitute "reasonable steps" that must be taken for compliance purposes. Other jurisdictions with similar regimes are facing comparable questions, which suggests that formal responsibility mapping alone is not sufficient.[53] Shifting organizational behavior requires clear standards, credible enforcement, and institutional commitment.

We recommend a modified certification approach for significant information economy actors that addresses the concerns raised about the UK system. A new law should require senior managers at covered companies to file Statements of Responsibilities with any agency with enforcement authority over the company's activities, products, or services. Covered companies should be required to certify the individuals responsible for certain key functions. Possibilities include "user engagement," "child and elder safety," or "bias and discrimination mitigation," to name only three. Responsibility mapping

---

46 *Senior Managers and Certification Regime*, Financial Conduct Authority (Feb. 13, 2026), https://www.fca.org.uk/firms/senior-managers-certification-regime.

47 *Id.*; Anat Keller & Andreas Kokkinis, *The Senior Managers and Certification Regime in Financial Firms: An Organisational Culture Analysis*, 22 J. Corp. L. Stud. 299 (2022); Elise Bernlohr Maizel, *Illegal Corporate Cultures*, 75 Duke L.J. 1 (2025).

48 *Senior Managers and Certification Regime, supra* note 46.

49 *Id.*

50 *Id.*

51 *Id.*

52 *See, e.g.*, Eleanore Hickman, *Is the Senior Managers and Certification Regime Changing Banking for Good?*, 85 Modern L. Rev. 1440 (2022); Nicholas Ryder et al., *Review of the senior managers & certification regime*, 2 J. Econ. Criminology 1 (2023).

53 Eleanore Hickman & Alan Brener, *The Senior Managers and Certification Regime in UK practice and global context*, 26 J. Banking Regul. 356 (2025).

should be paired with credible enforcement mechanisms, such as personal fines and time-limited or lifetime bars from working again in a particular role or industry. Enforcers can use these statements of responsibilities and certifications together with the accountability autopsies described above as starting points for their investigations. In cases involving serious harm and foresight, the people designated as responsible to guard against that category of harm may be named individually in the enforcers' complaints.

Operationalizing Coordinated Public Enforcement

Part 2 discussed why we favor cooperation and competition between multiple specialized enforcers over centralizing power in one information economy enforcer. The FTC too often stands alone as the general information economy regulator of last resort. Here, we recommend measured but effective ways of beefing up the enforcement footprint for other agencies, both to leverage their specialized expertise and to provide more opportunities for productive cooperation and competition.

To begin, Congress should close the loopholes that allow some companies to avoid narrowly defined sectoral regulation. Such companies compete with regulated rivals and subject their users and customers to the risks of harm a regulator is charged with policing, yet fall outside sectorally drawn lines. As one example, "buy now, pay later" providers like Klarna and Affirm function like credit cards from the consumer's point of view, but because the arrangements they offer are technically installment plans rather than extensions of credit, they may not be subject to the Truth in Lending Act's consumer protections. The CFPB's 2024 attempt to close this gap through an interpretive rule was withdrawn after the change of party control in 2025, demonstrating the need for more systematic thinking about how to craft legislative grants of authority that cannot be so easily avoided.[54] For example, Congress might redefine jurisdiction around categories of information ("health information") or uses of information ("health monitoring") rather than rigidly delineated business models ("hospitals").

Most of the companies that will be covered by a new regulator under these amendments will also be covered by the FTC's section five "unfair and deceptive acts and practices" (UDAP) requirements, creating the predicate for the kind of coordinated decentralization we recommend. Companies will be subjected to the overlapping but nonidentical requirements of two sets of regulatory obligations, and the oversight of regulators with different investigative and remedial tools, priorities, and areas of expertise.

At the same time, overlapping enforcement authority can increase transaction costs, delay action, and discourage information sharing. To address these concerns, agencies should adopt deconfliction mechanisms, perhaps borrowing from the DOJ/FTC merger process.[55] When both agencies wish to investigate a merger, the clearance process requires interagency negotiations, potentially culminating in direct talks between the heads of the agencies. Additionally, the FCC is consulted in telecom industry mergers, the Department of Transportation reviews mergers between airlines, and the Federal Reserve reviews bank mergers. Similarly when the FTC and CFPB, say, want to investigate or bring charges against a company for a single transaction or product design, the agencies may consult and cooperate to avoid unnecessarily duplicative actions.

54 Karl E. Schneider, Cong. Rsch. Serv., R48858, Buy Now, Pay Later: Policy Issues and Options for Congress (2026).

55 U.S. Gov't Accountability Off. GAO-23-105790, Antitrust: DOJ and FTC Jurisdictions Overlap, But Conflicts are Infrequent (2023), https://www.gao.gov/assets/820/814486.pdf.

Overseeing Accountable Enforcement

To bring greater accountability to enforcement, we propose creating a new Office of Enforcement Accountability (OEA). In our previous reports, we have recommended the creation of new hubs for cross-agency oversight and coordination three times: (1) a Digital Architectures, Systems, and Platforms Oversight Board (DASPOB) charged with developing standards for regulatory monitoring of information-economy activities, including especially those performed by digital platforms, and releasing data to the public; (2) a Department of Technology charged with supporting the development and, where necessary, the procurement of digital tools and systems for government use; and (3) an Office of Government Integrity to oversee and extend the capabilities of agency inspectors general (IGs). Once again, we aim to strike a balance. On one hand, it is important to build on carefully developed specialization and expertise. On the other, it is equally important to understand that many of the problems we are currently confronting require new thinking about building and implementing cross-agency capabilities.

The OEA is designed to fill a specific oversight gap: while IGs can and occasionally do examine enforcement-related actions, their focus on waste, fraud, and abuse and their resource constraints limit the extent to which they can produce enforcement-specific accountability. The OEA would have a narrower mandate to identify systemic patterns of underenforcement, overenforcement, or other politically influenced enforcement behavior. It would have authority to review open and closed enforcement actions, access investigative files, and inquire into decisions not to enforce. It would report directly to Congress, and agency leadership would be obligated to respond publicly to its concerns. Critically, the OEA would have no authority to intervene in ongoing actions or approve contemplated ones. In extraordinary cases of significant or repeated underenforcement, it could refer the matter to a state attorney general with jurisdiction over the underlying corporate conduct.

Finally, in a time of calls for federal preemption of new state laws, Congress should instead welcome state enforcement of the federal laws governing the information economy. New federal legislation–for example governing automated decisionmaking, comprehensive data protection, or the protection of minors online–should authorize state attorneys general to enforce the laws in state courts.[56]

---

56 Margaret H. Lemos, *State Enforcement of Federal Law*, 86 N.Y.U. L. Rev. 698 (2011).

Conclusion

This concept paper proposes essential means to bolster the enforcement of the laws that govern the information economy. By equipping agencies to treat design as a regulatory lever and ensuring that the individuals who architect harm face personal liability, we can more directly target the corporate practices and institutional structures that currently insulate information economy actors from meaningful accountability. By moving from the detect-investigate-prosecute model to a system of permanent, competitive oversight that matches the scale and permanence of the largest information economy actors, we can create a regime of direct, structural deterrence of wrongdoing.

Bibliography

Limits of Enforcement and Oversight

Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance,* 72 Vand. L. Rev. 1563 (2019).

Max J. Minzner, *Should Agencies Enforce?*, 99 Minn. L. Rev. 2069 (2015).

David Freeman Engstrom, *Agencies as Litigation Gatekeepers*, 123 Yale L.J. 616 (2013).

Chris Brummer, et al., *Regulation by Enforcement*, 96 S. Cal. L. Rev. 1319 (2023).

Rachel E. Barkow, *Overseeing Agency Enforcement,* 84 Geo. Wash. L. Rev. 1129 (September 2016).

David L. Markell & Robert L. Glicksman, *A Holistic Look at Agency Enforcement*, 93 N.C. L. Rev. 1 (2014).

Emily R. Chertoff & Jessica Bulman-Pozen, *The Administrative State's Second Face*, 100 N.Y.U. L. Rev. 727 (2025).

Verity Winship & Jennifer K. Robbennolt, *Admissions of Guilt in Civil Enforcement,* 102 Minn. L. Rev. 1077 (2018).

M. Elizabeth Magill, *Agency Choice of Policymaking Form*, 71 U. Chi. L. Rev. 1383 (2004).

Institutional design, enforcement incentives, and resource constraints

Jodi L. Short, *The Politics of Regulatory Enforcement and Compliance: Theorizing and Operationalizing Political Influences*, 15 Reg. & Governance 653 (July 2021).

Brian J. Broughman & Matthew T. Wansley, *Risk-Seeking Governance*, 76 Vand. L. Rev. 1299, 1342 (2023).

Hilary J. Allen, *Putting the Financial Stability in Financial Stability Oversight Council,* 76 Ohio St. L.J. 1087 (2015).

Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 Tex. L. Rev. 15 (2010).

Corporate and individual liability

Kimberly Kessler Ferzan, *Probing the Depths of the Responsible Corporate Officer's Duty*, 11 Crim. L. & Phil. 455 (2018).

Samuel W. Buell, *Criminally Bad Management* in Research Handbook on Corporate Crime and Financial Misdealing (J. Arlen ed. 2018)

Samuel W. Buell, *The Responsibility Gap in Corporate Crime*, 12 Crim. L. & Phil. 471 (2018)

Sean Lyness, *Revitalizing the State Environmental Responsible Corporate Officer Doctrine*, 64 Boston Coll.L. Rev. 253 (2023).

Anat Keller & Andreas Kokkinis, *The Senior Managers and Certification Regime in Financial Firms: An Organisational Culture Analysis*, 22 J. Corp. L. Stud. 299 (2022).

Elise Bernlohr Maizel, *Illegal Corporate Cultures,* 75 Duke L.J. 1 (2025).

Hannah Bloch-Wehba, *The Promise and Perils of Tech Whistleblowing*, 118 Nw. U.L. Rev. 1503 (2024).

Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. Cal. L. Rev. 383 (2017).

John C. Coffee, Jr., *"No Soul to Damn: No Body to Kick": An Unscandalized Inquiry into the Problem of Corporate Punishment*, 79 Mich. L. Rev. 386 (1981).

Remedial authority, redesign and other enforcement tools and reforms

Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018).

Daniel Wilf-Townsend, *The Deletion Remedy*, 103 N.C. L. Rev. 1809 (2025).

Elettra Bietti, *Experimentalism in Digital Platform Markets: Antitrust and Utilities' Convergence,* 2024 U. Ill. L. Rev. 1277 (2024).

Robert L. Glicksman, et al., *Technological Innovation, Data Analytics, and Environmental Enforcement*, 44 Ecology L.Q. 41 (2017).

Michael Asimow, Greenlighting Admin Prosecution (2022).

Brett Frischmann & Paul Ohm, *Governance Seams,* 36 Harv. J. L. & Tech. 1117 (2024).

Fragmentation and coordination in regulatory enforcement

Jacob Gersen, *Overlapping and Underlapping Jurisdiction in Administrative Law*, 2006 Sup. Ct. Rev. 201 (2007).

Jason Marisam, *Interagency Administration*, 45 Ariz. St. L.J. 183, 185–86 (2013),

Daniel A. Farber & Anne Joseph O'Connell, *Agencies as Adversaries*, 105 Cal. L. Rev. 1375 (2017).

Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space,* 125 Harv. L. Rev. 1131 (2012).

Margaret H. Lemos, *State Enforcement of Federal Law,* 86 N.Y.U. L. Rev. 698 (2011).

Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies),* 98 Cornell L. Rev. 769, 803 (2013).

Verity Winship, *Enforcement Networks*, 37 Yale J. on Reg. 274 (2020).


REDESIGNING THE
GOVERNANCE STACK
GEORGETOWN LAW