

INCOGNITO CONSUMER HARM

YUNSIEG P. KIM*

ABSTRACT

What good is a legal system built for visible injuries in a world where injury is designed to be invisible? This Article identifies and theorizes incognito consumer harm: consumer-facing wrongdoing that is intentionally designed, willfully or recklessly structured, or predictably allowed to remain unnoticed by most victims. A robot vacuum cleaner covertly records video inside consumers' homes. A seemingly helpful browser extension records everything users do on the internet. A dating advice app quietly retains photo IDs it promised to delete. In each case, the harm was exposed by an accident, a hack, or a whistleblower, not the legal system. In the status quo, hidden misconduct is too often exposed only after a system breach or an insider's disclosure, thus leaving victims at the mercy of wrongdoers to expose wrongdoing.

The existing legal system therefore fails doubly: It is not built to surface invisible injuries and, even when misconduct is exposed, current doctrine often fails to recognize concealed risk and informational deprivation as cognizable harms. Existing literature compounds the problem because even scholars who identify these harms as "invisible" overwhelmingly propose remedies that presuppose detection—the very thing that incognito harm prevents.

This Article argues that the status quo subsidizes concealment. The most successful wrongdoers, who should face the greatest accountability, face the least in practice because they are invisible. As AI increases firms'

* Associate Professor of Law, Maurice A. Deane School of Law at Hofstra University. J.D., Yale Law School; Ph.D., University of Michigan; M.S. in Cybersecurity, New York University Tandon School of Engineering. I thank Tiffany Chen, Ritika Gairola, Matthew Gaske, Daniel Greenwood, Sophie Klitgaard, Patrick Lin, Irina Manta, Shujin Meng, Andrew Miller, Sarah Parks, Sterling Reyes, Cassandra Burke Robertson, and Jack Zarin-Rosenfeld. I also thank the attendees of the 2025 Annual Meeting of the Midwestern Law & Economics Association and the 2026 Privacy Law Scholars Conference. I am grateful to the editors of the *Washington University Law Review* for their diligent and thoughtful work.

appetite for granular and intimate data, the undiscoverable extraction will yield greater payoffs. The solution to this problem is architectural: detection-first regulatory tools alongside litigation reforms that make concealment an aggravating factor instead of a liability shield.

TABLE OF CONTENTS

INTRODUCTION	266
I. DEFINING INCOGNITO CONSUMER HARM: CONCEPT AND SCOPE.....	270
A. <i>Definition and Representative Examples</i>	272
B. <i>Categories of Incognito Consumer Harm: Visibility and Culpability</i>	275
1. <i>Degrees of Invisibility: Fully Hidden, Partially Hidden, and De Facto Invisible Harms</i>	275
2. <i>Intentional, Willfully Blind, and Negligent Concealment</i>	277
C. <i>Incognito Consumer Harm and the Incomplete Contract Problem</i>	282
D. <i>Future Catalyst to Incognito Consumer Harm: Brandless Shopping</i>	283
II. WHY EXISTING LEGAL FRAMEWORKS FAIL TO ADDRESS INCOGNITO CONSUMER HARM.....	287
A. <i>Invisibility Evades the Detection Mechanisms of the Law</i>	288
1. <i>Litigation Requires Victims to See Invisible Harms</i>	288
2. <i>Spoliation Doctrine Is a Dead End</i>	290
3. <i>Regulatory Proposals: No “Alarm Bell” for Hidden Harms</i>	293
B. <i>Hidden Injuries Are Not Legally Recognized as “Harm”</i>	297
C. <i>Survivorship Bias Distorts the Law’s Perspective of Consumer Harm</i>	303
III. REFORMING THE SYSTEM: FROM DETECTION TO ENFORCEMENT.....	306
A. <i>Beyond Tweaks: Embracing a Detection-First Paradigm</i>	307
B. <i>Regulatory Reforms: Public Detection and Deterrence</i>	310
1. <i>Data Transparency Rights with Teeth</i>	310
2. <i>Telemetry and Mandatory Monitoring for Risky Systems</i>	313
3. <i>Proactive Audits and Whistleblower Incentives</i>	316
C. <i>Litigation Reforms: Unmasking Harm in Private Enforcement</i> ...	319
1. <i>Penalize Concealment-by-Design as Constructive Spoliation</i>	319
2. <i>Allow Limited Pre-Suit and Motion-Stage Discovery for Incognito Claims</i>	322
3. <i>Legislatively Make “Invisible” Injuries Actionable</i>	324
4. <i>Facilitate Aggregation and Representative Enforcement Without Rewarding Stealth</i>	326
D. <i>Minor vs. Structural Reforms and Litigation vs. Regulation: A Synthesis</i>	330
CONCLUSION	332

INTRODUCTION

How does the legal system learn that consumers are being harmed? In many cases, wrongdoers are exposed by other wrongdoers or sheer accident. An anonymous source¹ discovers that a browser extension records everything users do online, including which hotel rooms they book and which videos they watch,² because the extension left its source code publicly exposed.³ A consumer who “hooked up his . . . [robot] vacuum cleaner to his [PlayStation 5] controller” accidentally gains control of 7,000 robot vacuums like his and discovers “[l]ive camera feeds [and] microphone audio . . . across 24 countries.”⁴ Hackers breach a dating advice app’s servers and expose the users’ photo IDs, even though the app had publicly promised to delete the information immediately after verifying users’ identities.⁵ In each case, the harm was exposed by an accident, a breach, or a hack, instead of any proactive detection provided by the existing legal system. This Article names and theorizes the phenomenon that makes such mishaps necessary in the status quo: incognito consumer harm—consumer-facing wrongdoing that is intentionally designed, willfully or recklessly structured, or predictably allowed to remain unnoticed by most victims. When harm is engineered to be invisible, victims cannot sue or complain because they do not know that they were wronged, and the law remains oblivious while injury continues unabated.

1. MEGALAG, *Exposing Honey’s Evil Business Model (PART 2)*, at 00:25 (YouTube, Dec. 21, 2025), <https://www.youtube.com/watch?v=wwB3FmbcC88> (last visited June 5, 2026) (discussing how an “anonymous source found the code and sent it” to MegaLag).

2. Benjamin Altpeter, *More Than Just Coupon Codes: Browser Extension Honey Also Collects Their User’s History Data*, DATAREQUESTS.ORG (Nov. 2, 2020), <https://www.datarequests.org/blog/honey-data-collection/> [<https://perma.cc/7T9E-7CWE>] (discussing how Honey collected browsing history data at a large scale, “contrary to what their own privacy policy says,” including that “Honey knows . . . [o]n March 23 at 5 PM, [a user] watched the documentary ‘Scanning The Pyramids’ via the streaming provider CuriosityStream” and looked for “a hotel room for two adults for . . . March 04 to March 05”).

3. MEGALAG, *supra* note 1, at 00:19 (“Honey had left their source code exposed within their iOS app.”).

4. *The Accidental Hacker: How One Man Gained Control of 7,000 Robots*, GUARDIAN (Feb. 24, 2026, at 12:12 ET), <https://www.theguardian.com/lifeandstyle/2026/feb/24/accidental-hacker-how-one-man-gained-control-robots-> [<https://perma.cc/DDR7-8JMR>].

5. Isabella Kwai, *What to Know About the Hack at Tea, an App Where Women Share Red Flags About Men*, N.Y. TIMES (July 26, 2025), <https://www.nytimes.com/2025/07/26/us/tea-safety-dating-app-hack.html> [<https://perma.cc/NZ8E-HD8V>] (discussing how hackers obtained about 13,000 selfies and identification-document images despite Tea’s policy stating that verification selfies are deleted shortly after verification). As for this Article’s description of Tea as a dating advice app, the Apple App Store calls the app “Tea Dating Advice Inc.” *Tea Dating Advice Inc.*, APPLE APP STORE, <https://apps.apple.com/us/developer/tea-dating-advice-inc/id1654760315> [<https://perma.cc/LW7R-M63Z>].

While harming unsuspecting victims is not new, incognito consumer harm is novel and formidable for three reasons. First, modern technology has made concealment scalable, continuous, and embedded in everyday products. While technology did not invent concealment, it nevertheless enables remote, covert, continuous, and automatic extraction against millions of consumers. Today's consumer devices—dense with sensors and opaque intermediaries⁶—often collect intimate data as a condition of use. In 2025, Meta introduced a feature that it called “camera roll cloud processing” intended to help users come up with “creative ideas,” which would actually scan photos stored on local devices (such as smartphones) that users had not shared.⁷ The euphemism for such an invasive feature illustrates how firms are obfuscating the distinction between “functionality” and “extraction.”

Digital interfaces introduce novel ways to “optimize” concealment and extraction that were impossible in analog markets. Platforms can perform repeated A/B testing against specific demographic groups to determine which choice of words, default settings, or displays of terms of service is the most likely to suppress consumer awareness while extracting consent with the least friction.⁸ Concealment has become scalable and experimentally refinable, even as it masquerades as ordinary use.

Second, incognito consumer harm exposes a structural weakness in U.S. consumer protection neglected by existing literature. U.S. consumer protection law is often understood as a mix of public and private enforcement, in which agencies police unfair and deceptive practices while consumer litigation allows private enforcement and recovery.⁹ But courts cannot litigate the invisible, and agencies do not routinely audit products for concealed design choices. While such a system works for conspicuous harms—injuries that are immediate, legible, and traceable—it cannot work against injuries designed not to be noticed. Worse, the law's perspective of

6. See, e.g., Sylvia Lu, Note, *Data Privacy, Human Rights, and Algorithmic Opacity*, 110 CALIF. L. REV. 2087, 2120 (2022) (discussing how AI-driven consumer tools operate as opaque “black box” systems that invisibly monitor and decide, thus hindering oversight).

7. Gretchen Oestreicher, *How to Turn Off Meta AI: Facebook, Instagram, and WhatsApp*, METRICOOL (July 8, 2025), <https://metricool.com/opt-out-meta-ai-training/> [https://perma.cc/L2VA-KCK4] (explaining that the button to block or unblock Meta from “uploading [photos] from your device to Meta's servers” says “[g]et creative ideas made for you by allowing camera roll cloud processing”).

8. See, e.g., Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROCS. ACM ON HUM.-COMPUT. INTERACTION 81 (2019); see also Complaint at 25–29, *FTC v. Amazon.com, Inc.*, 735 F. Supp. 3d 1297 (W.D. Wash. 2024) (No. 2:23-cv-00932) (alleging that Amazon used iterative design testing to make it difficult to cancel Prime subscriptions).

9. See, e.g., Stephanie Bornstein, *Public-Private Co-Enforcement Litigation*, 104 MINN. L. REV. 811, 812 (2019) (“Federal statutes in . . . consumer . . . protection . . . include . . . ‘hybrid’ enforcement schemes . . . in which Congress created both public and private mechanisms for enforcing the law by establishing both a federal government agency and a private right of action with incentives to encourage citizen litigation.”).

consumer harm becomes systematically biased because it sees only the harms that it detects and mistakes that conspicuous subset for the whole universe of consumer injuries.¹⁰

Third, incognito consumer harm reveals a diagnosis-cure mismatch pervading the existing literature. More scholars are recognizing that modern consumer harms, increasingly mediated by algorithms, opaque systems, and pervasive data collection, can be hard to perceive. But even when scholars recognize such harms as “invisible,” they consistently propose remedies which first require exogenous detection. Professor Mark Lemley urges the FTC to act more aggressively against exploitative data practices that consumers rarely detect, but he proposes no mechanism for the FTC to discover those practices in the first place.¹¹ Professor Andrew Miller proposes litigation reforms for “invisible” algorithmic profiling, but his reforms require precisely what incognito harm prevents: a plaintiff who knows enough to sue.¹² Scholars thus present incognito harm as a remedial problem, even though it is first and fundamentally a detection problem. Promises of compensation and deterrence are hollow if wrongdoing fails to trigger enforcement. In the rare instances when enforcement *is* activated, it is often thanks to accidents, leaks, or hacks.

The incentives to commit incognito consumer harm are compelling and growing. As AI training demands vast quantities of data and publicly available sources of high-quality data are exhausted,¹³ firms across industries face increasing pressure to extract granular and intimate information while concealing the extraction.¹⁴ Fundamental changes in consumer behavior, including the rise of “brandless shopping,” in which products are sold under disposable or meaningless brand names,¹⁵ further reduce the reputational costs of misconduct. Incognito consumer harm is

10. See *infra* Section II.C.

11. Mark A. Lemley, Essay, *Protecting Consumers in a Post-Consent World*, 77 STAN. L. REV. ONLINE 247, 254, 258 (2025) (calling for “the FTC to expand its authority over ‘unfair . . . acts and practices’ to reach certain privacy practices,” an example of which is “if you have already given your data to a company under a particular privacy policy, they may (and frequently do) unilaterally change what they do with the data they already have about you,” without proposing a mechanism to enable the FTC to know when such practices occur).

12. Andrew Miller, *Invisible Allies: Algorithmic Consumer Profiling and the Rise of New Group Harms*, 28 YALE J.L. & TECH. 522, 594 (2026) (proposing “aggregate litigation” as a solution).

13. See Nicola Jones, *The AI Revolution Is Running Out of Data. What Can Researchers Do?*, NATURE (Dec. 11, 2024), <https://www.nature.com/articles/d41586-024-03990-2> [<https://perma.cc/6PZ8-U2HZ>].

14. See Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 976–77 (2021) (“As the relentless pressures of the market and the demands of advertisers led companies to acquire ever-more detailed and granular data, . . . market forces actively encourage [surveillance of consumers] in ways that are highly profitable . . .”).

15. See *infra* Section I.D.

therefore not the work of a few bad actors but instead a near universal strategy: Harvest what consumers cannot see because what they cannot see, they cannot challenge.

This Article argues that incognito consumer harm demands fundamental reform, rather than the marginal tweaks within existing law that the current literature overwhelmingly proposes.¹⁶ The problem is a structural failure resulting from a mismatch between new harms and old rules, in two respects. First, existing law is not built to detect invisible injuries. Litigation and regulation depend on victims or the public to notice harm and sound the alarm, an assumption that no longer holds when harm is engineered to evade notice. Second, even when incognito harm is exposed inadvertently, existing doctrine often lacks the vocabulary to treat it as a cognizable injury—especially when the harm takes the form of concealed risk, loss of control, or informational deprivation as opposed to immediate monetary loss. The fact that hidden harms occur more often than they used to is only a symptom. The ailment is that a system built for visible injuries cannot work in a world where injuries are designed to be invisible. Existing works’ proposed fixes inherit the same structural deficiency because they incorrectly assume that the system can already find what it needs to. Without detection-first reform, we will keep learning about hidden misconduct the way we do now: by accident, when a system gets hacked or an insider decides to talk.

This Article proceeds as follows. Part I defines incognito consumer harm and delineates its scope. It develops a taxonomy distinguishing degrees of invisibility (fully hidden, partially hidden, and de facto invisible harms) as well as degrees of culpability (intentional concealment, willfully blind or reckless invisibility, and negligent failure to create notice). These distinctions, which determine the appropriate detection strategy and legal culpability for incognito consumer harm, illustrate what the existing regime is structured not to see. Part II explains why existing legal frameworks fail even when we know what incognito consumer harm looks like. The failures are twofold and reinforcing. Invisibility erodes the law’s detection mechanisms, and existing doctrine’s narrow definition of injury disqualifies hidden harms even when they are eventually uncovered. These failures produce a survivorship bias in which the law sees only visible harms and mistakes that subset for the full universe of consumer injury. Part III

16. See, e.g., Lemley, *supra* note 11, at 248 (arguing that the FTC should use its existing powers to regulate “corporate abuse of notice and consent . . . in a range of competition and consumer protection cases”); Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1573 (2019) (advocating that the FTC use its “dormant statutory monitoring authority” for consumer protection).

proposes reforms that match the problem's structure: detection-first strategies upstream and litigation tools that penalize concealment downstream. I conclude by stressing that, without fundamental reform, the legal system will continue to function as a subsidy for concealment: strict on paper, but permissive and blind to the harms that it was built to prevent in practice.

I. DEFINING INCOGNITO CONSUMER HARM: CONCEPT AND SCOPE

Incognito consumer harm is not simply the latest incarnation of an old problem. Harming unaware victims is, of course, not new. A corporation might secretly dump toxic waste in a water source, harming anyone who drinks from it for years without their knowledge.¹⁷ Landlords have violated rent stabilization laws in ways that most tenants never discover.¹⁸ A hospital could commit malpractice that its patients do not realize for years.¹⁹ But these familiar examples differ from incognito consumer harm in two ways that existing scholarship has failed to appreciate, and this failure has led scholars to propose solutions that are systematically inadequate.

The first distinctive feature of incognito consumer harm is that technology has transformed even familiar forms of consumer-facing misconduct into a qualitatively different problem that transcends a change of mere degree. We have long understood that speed and scale alone can change an activity's fundamental character. The printing press only mechanized the manual task of copying books,²⁰ but it made production so much cheaper and faster that it broke the intelligentsia's "monopoly over common knowledge."²¹ Today, digital tools let firms inflict covert harm on

17. See, e.g., Wendy E. Wagner, *Commons Ignorance: The Failure of Environmental Law to Produce Needed Information on Health and the Environment*, 53 DUKE L.J. 1619, 1644 n.76 (2004) ("The difficulty of catching parties who secretly dump hazardous wastes on the property of others . . . led Congress to create an exclusion for owner liability under CERCLA.").

18. See, e.g., Justin R. La Mort, *The Theft of Affordable Housing: How Rent-Stabilized Apartments Are Disappearing from Fraudulent Individual Apartment Improvements and What Can Be Done to Save Them*, 40 N.Y.U. REV. L. & SOC. CHANGE 351, 362 (2016) (discussing how renters are often unaware that their apartments have been unlawfully deregulated and therefore do not challenge the resulting illegal rent increases).

19. See, e.g., David L. Abney, *For Whom the Statute Tolls: Medical Malpractice Under the Federal Tort Claims Act*, 61 NOTRE DAME L. REV. 696, 699 (1986) ("[V]ictims of medical malpractice . . . may be unaware for many years that they have been injured tortiously . . .").

20. See Stacey M. Lantagne, *Building a Better Mousetrap: Blocking Disney's Imperial Copyright Strategies*, 12 HARV. J. SPORTS & ENT. L. 141, 145 (2021) ("Before the printing press . . . , reproduction [generally] happened by hand, transcribed by monks in monasteries.").

21. TAYLOR W. BULEY, *THE FRESH POLITICS READER: MAKING CURRENT EVENTS AND PUBLIC AFFAIRS RELEVANT TO YOUNG AMERICANS* 272 (2006).

thousands or millions simultaneously,²² making incognito consumer harm a form of technology-assisted ambush: harder to anticipate, harder to detect, and incomparably more formidable than its analog predecessors.

Yet law and scholarship are slow to recognize the legal significance of this transformation. Scholars dismiss algorithmically accelerated wrongdoing as “old wine in new bottles” even though automation can compress a lengthy process into mere seconds.²³ The mental steps doctrine in patent law denies protection to inventions that speed up what a human could do “with a pen and paper,” even if they “add[] computer functionality to increase the speed or efficiency.”²⁴ This reflexive dismissal of technological acceleration pervades the legal system’s treatment of incognito consumer harm. When a “tiny middleman” can intercept a “million messages” carrying passcodes in a single month,²⁵ the claim that nothing has fundamentally changed amounts to denial or analytical failure.

The second distinguishing feature of incognito consumer harm is that scholars and regulators have focused on classifying *what* technology-assisted harms look like, while neglecting *how* those harms remain hidden. This distinction is critical, because knowing what a harm looks like is of limited practical value if the legal system cannot tell when it occurs. Former FTC Commissioner Rebecca Kelly Slaughter has written what she calls “a baseline taxonomy of algorithmic harms,” which she recognizes are generally invisible to consumers because algorithms can give a “false impression that these problems do not . . . exist.”²⁶ However, Slaughter’s taxonomy tracks sources of harm such as bad input data, flawed

22. Ryan Gallagher, Crofton Black & Gabriel Geiger, *How a Tiny Middleman Could Access Two-Factor Login Codes from Tech Giants*, BLOOMBERG (June 16, 2025, at 06:00 CT), <https://www.bloomberg.com/news/articles/2025-06-16/two-factor-authentication-codes-take-insecure-path-to-users> [<https://perma.cc/D3Z7-HBSC>] (discussing how Google, Amazon, and Meta send two-factor authentication passcodes by unencrypted SMS messages, which indicates that “[t]echnology companies are not doing good-enough due diligence on their own supply chain”).

23. Thibault Schrepel, *The Fundamental Unimportance of Algorithmic Collusion for Antitrust Law*, JOLT DIG. (Feb. 7, 2020) (citing Thibault Schrepel, *Collusion by Blockchain and Smart Contracts*, 33 HARV. J.L. & TECH. 117 (2019)), <https://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law> [<https://perma.cc/A79L-AYL6>] (discussing how algorithmic collusion is “old wine in new bottles” even though “algorithms could enable faster implementation of agreements between companies, potentially for only a few seconds,” because “[w]hether they are algorithmic or not, the nature of anti-competitive collusion remains identical . . . [and] algorithmic collusion is at the origin of two non-fundamental problems: detection, and liability assignment”).

24. *Cf.* *Ericsson Inc. v. TCL Comm’n Tech. Holdings Ltd.*, 955 F.3d 1317, 1327, 1330 (Fed. Cir. 2020) (declining to recognize a telecommunications patent because the claimed invention would merely do what can be done “by a human using a pen and paper”).

25. See Gallagher, Black & Geiger, *supra* note 22.

26. Rebecca Kelly Slaughter, Janice Kopec & Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. (SPECIAL ISSUE) 1, 1 (2021).

interpretations of outputs, and inadequate testing, instead of the mechanisms that conceal harm.²⁷ While such a focus is useful for understanding harm's causes, it does not help identify harm's *existence*. The absence of a concealment-centered framework also thwarts the design of solutions tailored to the many ways in which wrongdoers keep harm invisible. To address this oversight, Part I defines the concept of incognito consumer harm and illustrates its scope, so as to ground the theoretical and normative discussions that follow.

A. Definition and Representative Examples

Incognito consumer harm refers to consumer-facing harm intentionally designed, structured to avoid knowledge, or predictably allowed to go unnoticed by most victims, thereby bypassing the ordinary channels of awareness, complaint, and redress. Intentional concealment is the paradigm case, but the concept also reaches systems in which firms consciously avoid learning what their products are doing, or fail to build the notice, logging, and verification mechanisms that would make foreseeable injuries visible. In all three settings, the practical effect is the same: The consumer is deprived of the information necessary to object, exit, report, or sue. The perpetrator, often a company, profits from the hidden harm while consumers remain unaware that they have been injured. Classic examples include those discussed in the introduction. Tea, a popular dating advice app, asked users for selfies and photo IDs to verify identity and promised to delete the data after verification, but quietly retained the data for years.²⁸ Honey, a PayPal-owned browser extension that claims to find the best discounts for online shopping, recorded virtually everything users did online.²⁹ In each case, the perpetrator obtained something valuable—sensitive personal data or actionable behavioral insights—while consumers had no signal of harm. Indeed, both schemes were exposed by accident. Tea's deception surfaced only after hackers breached its servers and exposed the supposedly deleted photos and IDs,³⁰ and Honey's tracking came to light because "Honey had left their source code exposed within their iOS app" and an "anonymous source found the code and sent it" to an independent journalist for analysis and disclosure.³¹

27. See *id.* at 7–20.

28. See Kwai, *supra* note 5.

29. See Altpeter, *supra* note 2.

30. See Kwai, *supra* note 5.

31. See MEGALAG, *supra* note 1, at 00:19, 00:25.

Incognito consumer harm is not, in principle, limited to data and privacy. Any consumer-facing injury kept practically secret from victims through design, willful blindness, or failure to create reasonable mechanisms of notice can qualify, from social media influencers promoting products without disclosing paid sponsorship³² to landlords illegally raising rent on unaware tenants.³³ Across these contexts, the functional pattern is that the consumer remains deprived of the information needed to object, exit, report, or sue. This Article emphasizes data privacy examples because they expose two gaps in the literature with particular clarity. First, scholars often treat technology-enhanced incognito harm as mere acceleration of old misconduct—a distinction without a difference—even though technology-assisted scaling and automation make misconduct incomparably more formidable than before.³⁴ Second, scholars focus on the nature of the harm while paying too little attention to how the harm stays hidden, even as technology has multiplied both the means and the efficacy of hiding wrongdoing far beyond what was once imaginable.³⁵

Data privacy harms are therefore not the outer boundary of incognito consumer harm; they are its most instructive proving ground. The closest analog may be consumer finance, where scholars have long examined complexity, opacity, and cost structures that consumers do not readily understand or contest.³⁶ The relevant literature shows that invisibility predates AI or other contemporary technology. But incognito consumer harm is a distinct problem in both mechanism and institutional consequence. In consumer finance, the primary difficulty is that consumers misunderstand (or do not understand at all) the transaction they are engaging in. Incognito consumer harm goes further: the system itself often lacks meaningful audit trails, mechanisms for outside verification, or other ways for consumers and ordinary enforcement channels to know whether a violation even occurred. Put differently, consumer finance explains the legal significance of opacity; incognito consumer harm explains what happens when that opacity is deliberately engineered to prevent enforcement.

32. See David A. Hyman, David Franklyn, Leo Yang & Mohammad Rahmati, *Influencer Marketing on Instagram and TikTok: Entertainment or Deception?*, 22 VA. SPORTS & ENT. L.J. 154, 167 (2024) (discussing how many consumers are misled into thinking “that paid content is unpaid”).

33. See La Mort, *supra* note 18, at 362.

34. See *supra* notes 23–24 and accompanying discussion.

35. See *supra* notes 20–22 and accompanying discussion.

36. See, e.g., Natasha Sarin, *Making Consumer Finance Work*, 119 COLUM. L. REV. 1519, 1519 (2019) (“[B]anks regularly levy hidden fees on consumers, obscuring the true cost of financial products.”); Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 433 (2021) (discussing “impenetrably complex financial products”).

Incognito harm must be distinguished from two concepts it superficially resembles: diffuse harm and latent harm. The distinction from diffuse harm is particularly instructive. Diffuse harm—say, a hidden monthly fee of 61 cents on millions of consumers³⁷—is characterized by individual injuries being so small that many victims notice but rationally decline to act. The canonical problem of diffuse harm is hence one of *motivation*: Victims see the injury but lack sufficient incentive to complain. Incognito consumer harm is different in kind, not degree. Perpetrators rely on victims never realizing what was taken or compromised, which means that invisibility lets firms extract significant value from each consumer, who cannot even consider whether to resist because she does not know of anything to resist. But existing literature continues to understand rational apathy as the primary obstacle to effective consumer protection.³⁸ Incognito consumer harm reveals a prior and more fundamental obstacle: For a large and growing class of injuries, consumers never even reach the apathy calculus.

Incognito harm also differs from latent injuries that surface years later. Latent injuries such as toxic exposure eventually produce symptoms or losses that trigger awareness and legal action, even if the delay spans years or decades.³⁹ Incognito harm, in contrast, remains concealed unless exogenous and fortuitous events like a breach or whistleblower revelation force it into view. Its defining feature is invisibility, which short-circuits the legal system's usual triggers: When victims never know that they were wronged, complaint-driven enforcement never activates. With the concept clarified, I proceed to categorize incognito consumer harm according to visibility and culpability.

37. Jon Brodtkin, *AT&T Sued over Hidden Fee that Raises Mobile Prices Above Advertised Rate*, ARS TECHNICA (June 24, 2019, at 15:22), <https://arstechnica.com/tech-policy/2019/06/att-sued-over-hidden-fee-that-raises-mobile-prices-above-advertised-rate/> [<https://perma.cc/J3DC-RSL7>] (discussing how the junk fee started at 61 cents a month in 2013 and became \$1.99 a month in 2019, whereupon a class action was brought).

38. See, e.g., James M. Treece, *Trademark Licensing and Vertical Restraints in Franchising Arrangements*, 116 U. PA. L. REV. 435, 444 n.21 (1968) (discussing how “the number of reported cases” likely underreports consumer harm “because litigation is seldom worth the trouble” to consumers); Yonathan A. Arbel & Roy Shapira, *Theory of the Nudnik: The Future of Consumer Activism and What We Can Do to Stop It*, 73 VAND. L. REV. 929, 949 (2020) (“[M]ost consumers [who were harmed] do not invest the time in complaining, even though complaining would be beneficial for society by facilitating better-informed regulations, helping the regulator warn other market participants”); Christopher R. Leslie, *The Significance of Silence: Collective Action Problems and Class Action Settlements*, 59 FLA. L. REV. 71, 115 (2007) (“[T]he rational class member will not bother to object to an inadequate settlement.”).

39. See, e.g., Paul Davis Fancher, Note, *To Have and Not Hold: Applying the Discovery Rule to Loss of Consortium Claims Stemming from Premarital, Latent Injuries*, 53 VAND. L. REV. 685, 687–88 (2000) (“The latency period for injuries caused by toxic substances can range from a few years to more than one generation. A person exposed to a toxic substance may not discover the resulting injury until after marriage because of these long latency periods.”).

B. Categories of Incognito Consumer Harm: Visibility and Culpability

Incognito consumer harms vary along two dimensions: how visible the harm is to consumers and enforcement actors and the wrongdoer's culpability in producing or preserving that invisibility. On the first dimension, some harms are fully hidden from consumers absent a breach, whistleblower, or accident. Others are partially hidden because a small subset of consumers or experts may be able to detect them. Still others are *de facto* invisible: Consumers may experience frustration or suspicion but lack the information needed to identify the practice, connect it to a legal violation, or trigger enforcement. On the second dimension, some firms deliberately conceal misconduct; others cultivate ignorance about what their systems are doing; still others negligently fail to create mechanisms of notice. These distinctions bear directly on how we should detect, deter, and punish such wrongdoing. Fully concealed harms require different detection strategies from harms that consumers experience but cannot articulate or legally diagnose, and intentional cover-ups warrant different treatment from cultivated ignorance or negligent omission. This section outlines each category of harm in turn and explains how these differences affect legal doctrine and enforcement.

1. Degrees of Invisibility: Fully Hidden, Partially Hidden, and De Facto Invisible Harms

Some misconduct is fully incognito, as no consumer is likely to discover it absent an extraordinary fluke, the classic case being privacy violations engineered to leave victims none the wiser. I have already discussed examples involving robot vacuum cleaners, the Tea dating advice app, and the Honey browser extension collecting sensitive data.⁴⁰ Consumers typically cannot detect these injuries themselves because, in fully incognito schemes, victims have no practical trigger to complain. Thus, the harm stays hidden unless an outsider or whistleblowing insider forces it into public view.⁴¹

Other incognito consumer harms are *partially* hidden, as they are not apparent to most victims but are discoverable in unusual circumstances. A small subset of consumers or an unlikely chain of events may bring the harm to light while the majority remains oblivious. For instance, algorithmic manipulation or discrimination can affect thousands unaware, but a researcher, journalist, or whistleblower who talks to a broad enough group

40. See *supra* notes 1–5 and accompanying discussion.

41. See *supra* notes 1, 4–5 and accompanying discussion.

of consumers may uncover the pattern. A classic example is the travel booking site Orbitz directing Mac users to costlier hotel options than Windows users.⁴² Most travelers would not know that they were being steered to higher prices because it would likely not occur to them that a website would show different hotel options depending on which brand of computer they used to access the same website. In contrast, those with the resources, time, and incentive to suspect and document such a disparity—for example, *Wall Street Journal* reporters—may be able to find out.⁴³ Beyond this example, scholars argue that sophisticated algorithmic targeting can create “invisible” classes of disadvantaged consumers who never realize that they are being profiled.⁴⁴ In such contexts or settings, the probability of discovery is low but not zero.

A third category is de facto invisibility. In these cases, consumers may sense that something is wrong, but they cannot identify the practice, connect it to a legal violation, or articulate the experience into a complaint. Dark patterns are an illustrative example. A consumer forced through a deliberately confusing cancellation process may know that the exercise is maddening, but she likely has no way to know that the design was optimized to suppress cancellations⁴⁵ and no reason to suspect anything other than run-of-the-mill bad product design. Even the rare consumer who does suspect manipulation is not much better off than the ignorant one. Research finds that users who notice attempted manipulation through interfaces often comply anyway, because pushing back is not worth the effort for any single interaction.⁴⁶ De facto invisibility is technically distinct from full ignorance and full awareness, as the consumer perceives the surface symptom while remaining oblivious to the underlying wrong. Nevertheless, for enforcement purposes, the outcome is identical to full invisibility in that the alarm is silent under both scenarios.

This visibility spectrum should affect enforcement design because even *partially* hidden harms undermine the central assumption underlying the existing enforcement system—that victims will notice injuries and come

42. Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, at 18:07 ET), <https://www.wsj.com/articles/SB10001424052702304458604577488822667325882> [<https://perma.cc/4K27-KEXU>].

43. *Id.*

44. Miller, *supra* note 12, at 527 n.2.

45. See, e.g., Kerstin Bongard-Blanchy et al., “I Am Definitely Manipulated, Even When I Am Aware of It. It’s Ridiculous!” – Dark Patterns from the End-User Perspective, 2021 DESIGNING INTERACTIVE SYS. CONF. 763, 763 (“[R]espondents, especially younger ones, often recogni[z]e the ‘darkness’ of certain designs, but remain unsure of the actual harm they may suffer.”).

46. See, e.g., Maximilian Maier & Rikard Harr, *Dark Design Patterns: An End-User Perspective*, 16 HUM. TECH. 170, 171 (2020) (describing users “accepting undesirable privacy settings due to the difficulty of changing them”).

forward.⁴⁷ One might respond that aggregate litigation could address this problem, because a single aware victim could file a class action, and the notice process would alert the rest. Indeed, many scholars point to aggregate litigation as the solution to partially hidden harms like algorithmic discrimination.⁴⁸ But this response requires at least one victim to discover the harm and act—the very scenario that incognito harm prevents. Part II explores why existing litigation and regulatory frameworks fail to close the detection gap across the full spectrum of incognito harms.

2. *Intentional, Willfully Blind, and Negligent Concealment*

Incognito consumer harm also varies by the perpetrator's state of mind behind the concealment. Invisibility is often intentional because perpetrators knowingly hide wrongdoing through falsifications (such as engineering a device to mask intrusive data collection) or omissions (such as obfuscating disclosures so that consumers stay unaware). Examples of falsification include Google telling users that tracking was “off,” while continuing to record users' movements and use location data for targeted advertising.⁴⁹ A form of knowing concealment short of outright falsification is deception by obfuscation. For example, Meta invites users to “[g]et creative ideas made for you by allowing camera roll cloud processing,” which bears no resemblance to what Meta actually does with that permission: Meta can scan private photos stored on the user's phone.⁵⁰

Between intentional and negligent concealment lies a third category that may account for a large share of incognito consumer harm in practice: willful blindness, or what might alternatively be called cultivated ignorance. Here, a company does not affirmatively engineer invisibility in the manner of Google's surreptitious location tracking or Meta's obfuscatory consent language. Instead, it structures its operations so as to avoid learning what its own systems are doing to consumers—preferring not to know, so that it

47. See, e.g., Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309, 1326 (2015) (“[Unconscionable, unfair, deceptive, and abusive acts and practices] enforcement today is largely complaint driven.”); Dee Pridgen, *The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws*, 81 ANTITRUST L.J. 911, 933 (2017) (“[P]rivate enforcement of . . . consumer protection statutes [is] a strong deterrent against deceptive business practices . . .”).

48. See, e.g., Miller, *supra* note 12, at 594; Daniel Wilf-Townsend, *Artificial Intelligence and Aggregate Litigation*, 103 WASH. U. L. REV. 777, 777 (2026) (“Some AI injuries are . . . demonstrable only at the group level; others . . . may cause no actionable individual harm Aggregation creates opportunities to prove harm and assign remedies at the group level . . .”).

49. See Cecilia Kang, *Google Agrees to \$392 Million Privacy Settlement with 40 States*, N.Y. TIMES (Nov. 14, 2022), <https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html> [https://perma.cc/9TSG-KPG5].

50. See Oestreicher, *supra* note 7.

cannot be expected to fix what it does not know. The Supreme Court has recognized that willful blindness can be a basis for imputing knowledge when a defendant “subjectively believe[s] that there is a high probability that a fact exists” and “take[s] deliberate actions to avoid learning of that fact.”⁵¹ The Court applied that doctrine in the context of civil induced patent infringement, reflecting the traditional view that a willfully blind actor may be treated as comparably culpable to one with actual knowledge.⁵²

The distinction drawn here is behavioral and strategic, which are distinct from final liability. A firm that affirmatively engineers concealment, a firm that structures its organization to avoid learning what its systems do, and a firm that negligently fails to secure its infrastructure all present different challenges for detection. Granted, the fact that these firms would require tailored detection tools and the fact that the first two firms may ultimately face different sanctions from the third are correlated because the accused’s intention and knowledge go to both detection and punishment. But detection and punishment still demand different category distinctions because detection is an enforcement problem and punishment raises questions that are closer to the realm of jurisprudence.

In the incognito consumer harm context, willful blindness manifests when firms delegate consumer-facing decisions to algorithmic systems and, when consumers are harmed, the firm disclaims liability by claiming that it did not direct or even observe what the algorithm did. Consider a hypothetical company using a pricing algorithm that charges higher prices only to consumers in minority neighborhoods. The company might claim that the harm was not fully “deliberate” because it never asked for that result. But if the company chose not to audit the algorithm’s distributional effects—or went further and structured itself so that no employee could have observed them—calling the resulting invisibility an “accident” would strain credulity. The underlying concept is not new to the common law. A long line of “see no evil” cases holds that a defendant who “takes steps to make sure that he does not acquire full or exact knowledge” can be treated as though he knew it.⁵³

This middle category is where the strongest incentives for incognito consumer harm may lie. If incognito harm were exposed, intentional

51. *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011).

52. *Id.* at 766, 768–70 (discussing how willfully blind defendants are traditionally treated as “just as culpable as those who have actual knowledge” in the context of induced patent infringement under 35 U.S.C. § 271(b)).

53. *See, e.g., In re Aimster Copyright Litig.*, 334 F.3d 643, 650 (7th Cir. 2003) (“Willful blindness is knowledge, in copyright law . . . as it is in the law generally. . . . One who, knowing or strongly suspecting that he is involved in shady dealings, takes steps to make sure that he does not acquire full or exact knowledge . . . of those dealings is held to have a criminal intent.”).

concealers would face the highest penalties, and negligent firms could plausibly claim good faith. The willfully blind firm occupies the strategic sweet spot: It captures the benefits of invisibility while maintaining the defense that it did not “know” what its systems were doing. A taxonomy that lacks this middle category because it treats cultivated ignorance as mere negligence or requires proof of affirmative direction to call it intentional would distort the law’s picture of consumer-facing harm by systematically undercounting only a particular subset of it.

In contrast, some harms are incognito through negligence. A company did not *set out* to hide the injury, but its lack of care resulted in consumers never being informed. Here, the perpetrator’s fault is in carelessness or incompetence rather than trickery. For example, a company’s sloppy security practices might allow a breach that goes undetected for months, during which time consumers’ personal information is quietly stolen without their knowledge. In 2021, T-Mobile suffered a breach in which “names, addresses, . . . and Social Security numbers” of more than fifty million consumers were stolen after a hacker found “an unprotected router” in T-Mobile’s network.⁵⁴ Here, the harm’s invisibility is due to poor corporate practices rather than a deliberate cover-up. The company may eventually come clean once the issue comes to light, but until then, the effect on consumers is the same as in intentional cases: They are unaware of the ongoing injury. In the case of T-Mobile, the hacker claimed responsibility for the hack by speaking to the *Wall Street Journal*.⁵⁵ Had the hacker chosen silence over self-promotion, the compromise of over fifty million consumers’ personal information might have remained undetected indefinitely. This example illustrates that even negligent incognito harm often depends on fortuity, not on the legal system’s detection capacity, for its eventual exposure.

The lines among intentional concealment, willful blindness, and negligence are not always clear at the time of exposure. Tea publicly promised to delete users’ verification data but retained it for years,⁵⁶ which

54. See Jonathan Stempel & Sara Merken, *T-Mobile to Pay \$350 Mln in Settlement over Massive Hacking*, REUTERS (July 22, 2022, at 17:53 CT), <https://www.reuters.com/business/media-telecom/t-mobile-pay-350-mln-settlement-over-massive-hacking-2022-07-22/> [<https://perma.cc/86DQ-N55B>].

55. See Drew FitzGerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: ‘Their Security Is Awful,’* WALL ST. J. (Aug. 27, 2021, at 18:36 ET), <https://www.wsj.com/business/telecom/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105> [<https://perma.cc/84UB-8BAP>].

56. Tammana Malik, *Safest Space to Spill the Tea?: “Dating Safety” App Targeted in Massive Data Breach*, NAT’L L. REV. (July 28, 2025), <https://natlawreview.com/article/safest-space-spill-tea-dating-safety-app-targeted-massive-data-breach> [<https://perma.cc/LL7F-VDR4>] (quoting Tea’s 2022 privacy policy, which states that verification photos are “securely processed and stored only temporarily and will be deleted immediately following the completion of the verification process”).

facially appears to be intentional concealment. But Tea has claimed both that the data sat in a legacy system which was not migrated to newer infrastructure and that the data were intentionally archived to comply with law enforcement requirements related to cyberbullying prevention.⁵⁷ If the former is true, the case is closer to T-Mobile's negligent failure to secure a router; if the latter is true, the data retention was deliberate but recharacterized after the fact as having a legitimate purpose. There is, of course, the possibility that Tea simply chose not to investigate whether legacy data had been migrated or deleted. Such a case would be one of willful blindness, where the firm's fault lies in deceiving itself instead of others. In such ambiguous scenarios, intentional concealers could present intentional wrongdoing as innocent oversight. Detection-first tools could counter such plausible deniability with independent verification.

These culpability distinctions are consequential for enforcement design. The law typically calibrates sanctions to fault, and incognito consumer harm should be no different.⁵⁸ Intentional concealment and cultivated ignorance warrant stronger condemnation than, say, negligent failure to create notice, because both intentional concealment and cultivated ignorance allow firms to benefit from invisibility while avoiding ordinary accountability.⁵⁹ Negligent incognito harms, though still serious, are more plausibly understood as failures of diligence that do not present the same degree of moral culpability.⁶⁰ Deliberate concealment and cultivated ignorance should thus carry heightened penalties. A firm that inadvertently makes a harm invisible but voluntarily and promptly comes forward upon discovery is materially different—a difference that the law should recognize.

Culpability can also influence the doctrinal tools available. Some causes of action require intent or knowledge: Fraud, for instance, requires knowing

57. Press Release, Tea, Update Regarding Cybersecurity Incident (July 25, 2025), <https://www.classaction.org/media/tea-dating-safety-app-cybersecurity-incident.pdf> [https://perma.cc/P5F3-KNTW] ("This information was stored in accordance with law enforcement requirements related to cyber-bullying investigations. . . . During our early stages of development some legacy content was not migrated into our new fortified system. An unauthorized actor accessed our identifier link where data was stored before February 24, 2024.").

58. Cf. Justin V. Rodriguez, Comment, *Six Unconstitutional Homicide Statutes: Rational Basis Review and the Problem of Harsher Punishment for Less Culpable Offenders*, 158 U. PA. L. REV. 231, 232 (2009) ("The correlation of punishment to culpability stands firmly as the bedrock principle upon which legislatures construct criminal codes.").

59. Cf. Wes Henricksen, *Deceive, Profit, Repeat: Public Deception Schemes to Conceal Product Dangers*, 42 CARDOZO L. REV. 2395, 2425 (2021) ("Treating a purposeful wrong as negligence is akin to treating a premeditated killing as manslaughter rather than murder; it diminishes the wrongfulness of the act, very likely resulting in reduced culpability . . .").

60. Cf. *Wauchope v. Domino's Pizza, Inc.*, 832 F. Supp. 1577, 1579 (N.D. Ind. 1993) ("In actions arising under tort, mere negligence will not support an award of punitive damages.").

misrepresentation.⁶¹ Intentional incognito harms may support fraud claims or willful violation penalties, while willful blindness may, in appropriate regimes, satisfy knowledge-based requirements or justify treating ignorance as culpable rather than exculpatory.⁶² Negligent concealment may instead fall under failure-to-warn, negligent misrepresentation, or consumer protection theories that impose disclosure duties without requiring proof of deliberate deceit.⁶³ Intentional concealment and cultivated ignorance may also justify shifting burdens or presumptions where the defendant's conduct made proof unavailable.⁶⁴ Such doctrinal leeway may not extend to negligent concealment. But a firm that negligently left consumers in the dark can still be liable under consumer protection statutes that impose a duty to disclose material information.⁶⁵

In sum, parsing incognito harms by visibility and culpability illustrates why they are a uniquely difficult problem for existing law. Fully invisible harms engineered for secrecy present a nearly impenetrable challenge for traditional enforcement, like a tree falling in a forest with no one to hear; partially invisible harms can still exploit limited consumer awareness and persist for long periods; and de facto invisible harms where consumers perceive frustration or friction but cannot connect it to a cognizable wrong produce the same enforcement silence as full invisibility. Moreover, intentional concealment, willful blindness, and negligent omission represent meaningfully different wrongs. Intentional concealment attacks the transparency on which free markets and the law depend; willful blindness exploits the strategic middle ground between knowledge and ignorance; and negligence reflects a breakdown of corporate responsibility. Because the solutions and sanctions must differ across this spectrum, these categories go beyond merely refining terminology and justify this Article's central prescriptions: detection-first tools for fully incognito consumer harms and

61. See, e.g., *Unicolors, Inc. v. H&M Hennes & Mauritz, L.P.*, 595 U.S. 178, 188 (2022) ("Fraud typically requires '[a] knowing misrepresentation . . . of a material fact.'").

62. See *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 768–70 (2011) (discussing how induced infringement requires knowledge and applying the doctrine of willful blindness to satisfy that requirement).

63. See, e.g., *In re Allergan BIOCELL Textured Breast Implant Prods. Liab. Litig.*, 537 F. Supp. 3d 679, 735–51 (D.N.J. 2021) (discussing how negligent misrepresentation can enable failure-to-warn claims under the laws of various states).

64. See, e.g., *Lynch v. Saddler*, 656 N.W.2d 104, 111 (Iowa 2003) (explaining that an adverse inference "may only be drawn when the destruction of relevant evidence was intentional, as opposed to merely negligent").

65. See, e.g., Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, Comm. on Energy & Com., U.S. House of Reps. (Oct. 14, 1983), reprinted in *In re Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984) (explaining that deception may arise from a representation, omission, or practice likely to mislead reasonable consumers, and that the representation or omission must be material).

a direct legal reckoning with concealment itself, whether deliberate or willfully blind. Before discussing those reforms, Section I.C examines how incomplete contracts and illusory consent in modern consumer transactions create fertile ground for incognito harm enhanced by technology.

C. Incognito Consumer Harm and the Incomplete Contract Problem

While failures in consumer vigilance may contribute to the detection gap identified by this Article, they are far from the sole cause. The problem is compounded by a structural feature of modern consumer transactions: incomplete contracts that obscure what firms actually do with consumer assets like data, attention, and trust. Scholars have argued for decades that mass-market consumer agreements can amount to “lawful fraud”—standardized deals that leave crucial aspects of the exchange unspecified or obscured.⁶⁶ As scholars have also noted, boilerplate terms routinely gloss over what firms actually do, rendering consumer consent a thing of fiction.⁶⁷ Because of this information asymmetry, consumers unwittingly supply valuable inputs such as personal information and behavioral data that firms monetize through undisclosed secondary uses without any bargained-for compensation.⁶⁸ Thus, far from being mere background context for incognito consumer harm, incomplete contracts serve as part of the concealment mechanism itself by creating scenarios ripe for the exploitation of millions of consumers at the same time.

What makes the contemporary information asymmetry especially dangerous for incognito consumer harm is that it flummoxes both lay consumers and the experts meant to police it, such as judges and regulators. Digital products are designed to be intuitive, which lulls even sophisticated actors into thinking that they understand the underlying technology and contractual mechanics. As one study put it, “[t]echnology is often presented as a product that does not require technological expertise to use, and lawyers mistake their ability to use a product for understanding the underlying technology.”⁶⁹ This illusion of proficiency leads legal professionals to overestimate their grasp of complex digital systems without apprehending

66. See, e.g., W. David Slawson, *Mass Contracts: Lawful Fraud in California*, 48 S. CAL. L. REV. 1, 1–2 (1974).

67. See, e.g., Lemley, *supra* note 11, at 249 (“Even where privacy laws offer a nominal choice, companies circumvent it by making the sharing of data the easier option.”).

68. See, e.g., Richards & Hartzog, *supra* note 14, at 972–73 (“Human customers who trust tech companies become transformed into sources of the raw material,” which amounts to “opportunistic exploitation of human customers.”).

69. Yunsieq P. Kim, *The Faster Horse Fallacy: How the Law Idealizes Technology*, 2025 U. ILL. L. REV. 609, 613.

the novel risks and failure modes that these tools introduce. Federal courts assume that an email functions just like a letter, only faster and cheaper, even though companies abuse spam filters to avoid making required notices.⁷⁰ Scholars present technology-assisted discovery tools as “almost certainly better than humans in precision,” even though AI can make errors that human lawyers are far less likely to make.⁷¹ The result is a misperception at every level of the enforcement chain. If even the system’s gatekeepers cannot see through technological opacity, consumer protection is doing something much worse than underperforming: It is operating on a false picture of what is happening.

This misalignment leaves legal experts with a dangerous overconfidence in traditional remedies and a perception that consumer protection is working when it is not. Time and again, rules are enacted with no reliable means to verify compliance, effectively relying on the industry’s good faith.⁷² The result is a paper shield of a regulation that looks strict on its face but is toothless against hidden misconduct. Yet, neither scholars nor regulators have fully reckoned with the depth of this problem—namely, that it is not only consumers who are outmatched by technological complexity but also the institutional apparatus itself.

The incomplete contract problem thus deepens the detection gap in a way that the literature has not fully reckoned with. Information asymmetry, once largely a matter of fine print and hidden fees, has been supercharged by digital complexity to the point that even judges and regulators often cannot discern what is happening beneath the surface of familiar-looking products. The detection gap is therefore not a problem that consumer education can solve singlehandedly. It is a systemic failure that requires rebuilding the law’s capacity to verify what firms actually do, rather than taking at face value what they say they do. Before discussing those failures, Section I.D examines an emerging phenomenon that is compounding the detection gap by providing further cover for potential wrongdoers: brandless shopping.

D. Future Catalyst to Incognito Consumer Harm: Brandless Shopping

In addition to incomplete contracts and technological complexity, an even more basic layer of invisibility is emerging that further enables incognito consumer harm: Companies can increasingly conceal their very

70. *Id.* at 613–35.

71. *Id.* at 642–50 (citing David Freeman Engstrom & Jonah B. Gelbach, *Legal Tech, Civil Procedure, and the Future of Adversarialism*, 169 U. PA. L. REV. 1001, 1052–53 (2021)).

72. *See, e.g.*, N.Y. GEN. BUS. LAW § 349-a (McKinney 2026) (requiring firms to disclose any use of personalized algorithmic pricing without providing a means of verifying compliance).

identity from consumers. Historically, the need for brand recognition kept firms visible and accountable because corporate survival depended on being known and trusted by customers, which inherently limited the extent to which a firm could hide ongoing malfeasance.⁷³ However, a recent shift toward “brandless” shopping in e-commerce is eroding this traditional check. Major platforms now enable even the smallest sellers to market products in generic or disposable names, offering little to no consistent brand identity that consumers recognize or remember.⁷⁴ By severing the link between a product and any familiar producer, this trend makes it harder for consumers or regulators to trace harm back to its source, thereby greatly reducing the reputational and legal risks that would ordinarily help deter misconduct.

Although brandless shopping seems to have escaped the notice of legal scholars,⁷⁵ it is familiar to any halfway regular shopper on Amazon. “Open up a category on Amazon—Electronics, Toys, Home Garden & Tools, whatever—and scan the first page for a product listed with no obvious brand, or perhaps a semi-brand like IOCBYHZ, BANKKY, or KLAQQED”⁷⁶ instead of any manufacturer that typical consumers would have ever heard of. The following are two listings of the same product, a contraption to squeeze toothpaste tubes to their last ounce, sold under two different “brands” for the exact same price:

73. Cf. MARK BATEY, *BRAND MEANING: MEANING, MYTH AND MYSTIQUE IN TODAY’S BRANDS* 1–2 (2d ed. 2016) (“Brick makers in ancient Egypt are said to have put symbols on their bricks to identify them. In Europe the earliest signs of branding were the medieval guilds’ efforts to require craftsmen and craftswomen to put trademarks on their products to protect themselves and consumers against imitation and inferior quality.”).

74. Juozas Kaziukėnas, *Amazon Laid the Brandless Foundation for Temu*, MARKETPLACE PULSE (Oct. 10, 2024), <https://www.marketplacepulse.com/articles/amazon-laid-the-brandless-foundation-for-temu> [https://perma.cc/P5E3-PKMD] (“Amazon is a brandless retailer.”).

75. One such indication is that, as of January 5, 2026, a search on Westlaw using the term “brandless shopping” returned no documents. The only returned results (ten entries under the category “key number”) were all irrelevant to brandless shopping. WESTLAW, adv:“brandless shopping”, 10 results (Jan. 5, 2026) [https://perma.cc/K7VZ-SF7R].

76. John Herrman, *Is Amazon Turning into Temu? The E-Commerce Platforms Are Converging on the Same Plan: A Race to the Ultracheap Brandless Bottom*, N.Y. MAG. (Aug. 4, 2024), <https://nymag.com/intelligencer/article/is-amazon-turning-into-temu.html> [https://perma.cc/8Z55-ZH89].



77



78

This brandless model would be less harmful if Amazon reliably supplied the missing trust function. Many shoppers treat Amazon's brand and its customer review system as substitutes for individual company brands.⁷⁹ But Amazon's gatekeeping has been alarmingly lax. An estimated 42 percent of the 720 million Amazon product reviews assessed in 2020 were fake or

77. XYKEEY Set of 2 Toothpaste Squeezer Rollers, Metal Toothpaste Tube Wringer Seat Holder Stand (Stainless Steel), AMAZON, <https://www.amazon.com/Toothpaste-Tube-Squeezer-Rollers-Wringer/dp/B07SHL6P8V/?th=1> [<https://perma.cc/3DYH-LEY6>] (last visited June 6, 2026).

78. Toothpaste Squeezer - Metal Tube Squeezer Stainless Steel Tube Wringer UDQYQ Toothpaste Seat Holder Stand (Silver), AMAZON, <https://www.amazon.com/Toothpaste-Squeezer-Stainless-Wringer-Holder/dp/B085W1ZSBT/> [<https://perma.cc/6CNY-V9X4>] (last visited June 6, 2026).

79. Kaziukėnas, *supra* note 74.

manipulated,⁸⁰ and blatantly substandard or unsafe merchandise can maintain glowing ratings. Third-party sellers have offered electrical fuses and connectors that boast 4.7-star average reviews despite their alleged failures to prevent overloads, fires, or electrocution.⁸¹ Other reports describe nutritional supplements containing less than 2 percent of the advertised ingredient,⁸² banned sellers resurfacing with the exact same items under new aliases,⁸³ and sellers offering customers cash or gift cards for five-star ratings despite Amazon claiming to ban the practice.⁸⁴ Amazon has leaned into the “race to the ultracheap brandless bottom” with Haul, a discount storefront that “looks like a Temu version of Temu”⁸⁵ and sells brandless products such as “\$1 earrings and \$8 leggings.”⁸⁶ As for Temu itself, the online shopping site notorious for rock-bottom prices and no-name merchandise, it gained an astonishing 51.4 million users between September 2022 and January 2024 in the United States.⁸⁷

This Article’s taxonomy applies most naturally to direct perpetrators, but Amazon’s role raises a distinct question: how to classify the platform intermediary that creates conditions for incognito consumer harm without itself committing it. Amazon is not the seller offering unsafe fuses or

80. Press Release, Richard Blumenthal, U.S. Sen. for Conn., Blumenthal Calls on Amazon to Curb Rampant Fraudulent Reviews (Dec. 5, 2022), <https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-calls-on-amazon-to- curb-rampant-fraudulent-reviews> [https://perma.cc/A5VB-E52Y].

81. LOUIS ROSSMANN, *Amazon Sells Dangerous Electrical Crimps* (YouTube, Dec. 16, 2023), https://www.youtube.com/watch?v=y83BS_mK9GE (last visited July 15, 2026); LOUIS ROSSMANN, *Amazon Sells Fake Electrical Fuses* (YouTube, Dec. 30, 2023), https://www.youtube.com/watch?v=B90_SNNbcoU (last visited July 15, 2026).

82. Hank Schultz, *9 of 10 Amazon Galantamine Memory Supplements Failed to Meet Label Claim*, SUPPLYSIDE SUPPLEMENT J. (Feb. 23, 2024), <https://www.supplysidesj.com/supplement-regulations/9-of-10-amazon-galantamine-memory-supplements-failed-to-meet-label-claim-> [https://perma.cc/3X9P-G89J].

83. Matt Safford, *DeepCool Penalizes Chinese Distributor for Selling Sanctioned Products on Amazon in the US—Blurred Logo and Brand Name Change Violated Contract*, TOM’S HARDWARE (Aug. 30, 2024), <https://www.tomshardware.com/pc-components/cooling/deepcool-penalizes-chinese-distributor-for-selling-sanctioned-products-on-amazon-in-the-us-blurred-logo-and-brand-name-change-violated-contract> [https://perma.cc/6YPW-NEKB].

84. Lauren Victory, *Crystal Lake Man Raises Questions About Amazon’s Ban on Paid Reviews After Getting \$20 Offer for a 5-Star Review*, CBS NEWS (May 5, 2022, at 06:29 CT), <https://www.cbsnews.com/chicago/news/crystal-lake-man-raises-questions-about-amazons-ban-on-paid-reviews-after-getting-20-offer-for-a-5-star-review/> [https://perma.cc/373S-Q28P].

85. Katie Notopoulos, *Amazon’s New Discount Section, ‘Haul,’ Looks Like a Temu Version of Temu*, BUS. INSIDER (Nov. 14, 2024, at 15:48 CT), <https://www.businessinsider.com/amazon-haul-temu-shein-compared-which-is-better-worse-2024-11> [https://perma.cc/GAS7-HTW6].

86. Jason Del Rey, *Amazon Unveils ‘Haul’—Its Ultra-Discount Temu Rival Selling \$1 Earrings and \$8 Leggings*, FORTUNE (Nov. 13, 2024, at 12:30 ET), <https://fortune.com/2024/11/13/amazon-haul-temu-shein-discount-store-tiktok-shop/> [https://perma.cc/R6VS-X9ZH].

87. Yunsieg P. Kim, *Micromanaging Technology*, 29 YALE J.L. & TECH. (forthcoming 2026) (manuscript at 63), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5179546 [https://perma.cc/TK3R-RF44].

supplements containing 2 percent of the advertised ingredient. But its marketplace architecture—algorithmic ranking that rewards low price over verifiable identity and review systems that are demonstrably gameable—determines how easily bad actors can operate undetected. The launch of Haul suggests that at least some of this architecture reflects deliberate commercial strategy rather than mere inability to police scale. Whether Amazon’s posture is best understood as intentional enablement, willful blindness to the harms its architecture facilitates, or negligent gatekeeping, the enforcement priority does not change: If the platform that sets the marketplace’s rules is not held accountable for the detection gap that its design creates, reforming individual sellers’ behavior would be tantamount to treating the symptoms while the underlying condition persists.

For incognito consumer harm, brandless shopping is an accelerant. Incognito harm begins when consumers do not know that they were harmed. Brandless shopping compounds the problem: Even when harm is somehow detected, consumers may not be able to identify *who* harmed them. Branding once supplied an enforcement anchor by creating a traceable identity that regulators could target and plaintiffs could sue. When that anchor disappears, enforcement becomes harder at every stage, from investigation and service of process to collection of judgments. Should the brandless model continue to proliferate, the law’s focus on conspicuous, brand-linked wrongdoing will be looking at an ever-shrinking tip of the iceberg, while a growing mass of incognito harm remains submerged and unaddressed.

Brandless shopping shows that the problem of incognito consumer harm is both technological and institutional. The way that technology presents itself—frictionless and familiar—can mask how it actually operates and evolves beyond the law’s view, aided by consumer behavior. Confronting incognito harm thus requires revisiting legal assumptions built on symmetric information and stable products, and shifting enforcement toward mechanisms that can verify compliance instead of assuming it. Part I having defined and categorized incognito consumer harm, Part II explains why existing enforcement regimes as well as much of the literature fail to address it.

II. WHY EXISTING LEGAL FRAMEWORKS FAIL TO ADDRESS INCOGNITO CONSUMER HARM

Existing legal frameworks are ill-equipped to address incognito consumer harm in two compounding ways that the current literature has not fully appreciated. First, both litigation and regulation assume that someone

will notice and report the harm, an assumption that incognito harm subverts by design. Second, even when hidden harms do come to light, whether through a whistleblower or sheer accident, courts often struggle to recognize them as cognizable injuries. Doctrines like standing or pleading are built for visible harm and tend to dismiss risks or losses kept out of sight. Harm must therefore survive the first filter (detection) only to face the second (legal cognizability), and each filter independently screens out incognito harm. The result is both under-enforcement and a system that is structurally biased toward seeing only what it is already built to see.

Part II explores these twin failures. Section A discusses how invisibility evades the law's detection mechanisms. Section B shows how legal definitions of injury often exclude hidden harms, even when they are eventually detected. Section C synthesizes Sections A and B to show that deficient detection and definitions of injury create a survivorship bias: The law sees, and thus governs, only visible harms and mistakes them for the full universe of consumer injury.

A. Invisibility Evades the Detection Mechanisms of the Law

1. Litigation Requires Victims to See Invisible Harms

A prominent strand of recent scholarship treats litigation and procedural refinement as the primary solution to opaque, systemic consumer harms without explaining how those harms would be discovered in the first place. Professor Andrew Miller observes that algorithmic profiling can create “invisible” groups of disadvantaged consumers who might never realize that they were targeted.⁸⁸ He argues that litigation is crucial to uncovering “exploitation by powerful . . . marketplace actors” and proposes refining procedural tools such as class actions and multidistrict litigation.⁸⁹ Yet Miller highlights the catch-22 that his own argument represents: He relies on victims to sue even as he acknowledges that these consumers often do not know that they were harmed.⁹⁰ Without any mechanism to trigger a case in the first place, his litigation strategy risks helping only the rare victim who happens to notice.

Other works are afflicted by the same catch-22. Professor Nadiyah Humber urges reviving the Fair Housing Act's “discriminatory effects” standard to challenge tenant-screening tools that perpetuate “algorithmic

88. See Miller, *supra* note 12, at 552–53.

89. *Id.* at 600.

90. See *id.* at 567 (discussing “the importance of making visible” groups harmed by algorithms).

redlining.”⁹¹ But she concedes that more transparency would “allow declined tenants to seek redress,”⁹² implicitly acknowledging that many renters never realize that they were algorithmically screened out. Without ex ante measures to reveal hidden bias, even an expanded Fair Housing Act theory would remain mostly unused, reaching only the rare cases that happen to be discovered.⁹³

One might expect solutions based on aggregate litigation to suffice because class actions are designed specifically to overcome individual victims’ rational apathy. But the detection gap persists even in the most sophisticated aggregation proposals. Professors Peter Salib and Daniel Wilf-Townsend place class action litigation at the heart of their responses to opaque algorithmic injuries, yet both proposals inherit the same detection prerequisite. Salib argues that, after *Wal-Mart Stores, Inc. v. Dukes*, many “high-merit, but low-dollar” claims have little or no access to justice because they cannot meet class certification requirements.⁹⁴ *Wal-Mart* and its progeny disapproved of using statistics to establish commonality, effectively barring certain systemic bias cases from class actions.⁹⁵ The result, Salib argues, is that “untold numbers of meritorious claims . . . evaporate” absent an aggregation mechanism.⁹⁶ His solution is an AI jury that uses machine learning to resolve individualized issues in a class, thus satisfying predominance and making certification feasible for claims that would otherwise fail.⁹⁷ But even a perfectly functioning AI jury cannot deliver compensation or deterrence if no one realizes that they were wronged in the first place.

Wilf-Townsend comes closer to identifying the detection problem directly. He argues that “[s]ome AI injuries are statistically demonstrable only at the group level,” thus frustrating traditional individual claims,⁹⁸ and

91. Nadiyah J. Humber, *A Home for Digital Equity: Algorithmic Redlining and Property Technology*, 111 CALIF. L. REV. 1421, 1468–69 (2023) (“illustrat[ing] the benefits of segregative effect theory and its potential application to algorithmic redlining”).

92. *Id.* at 1430.

93. *See id.* at 1424 (using *Louis v. SafeRent Solutions, LLC*, 685 F. Supp. 3d 19 (D. Mass. 2023), to illustrate how “[l]andlords have long relied on imperfect proxies to turn down prospective tenants, [which] . . . very often track race”).

94. Peter N. Salib, *Artificially Intelligent Class Actions*, 100 TEX. L. REV. 519, 525 (2022).

95. *See id.* at 520–22 (discussing how *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011), rejected “new, creative, and certification-facilitating methods of statistical proof,” effectively raising the bar for certification across “whole categories of putative classes in a range of important doctrinal areas,” including class actions involving “consumer fraud”).

96. *Id.* at 521.

97. *See id.* at 524 (proposing to use actual jury determinations “to train an algorithm to mimic the jury’s decision function” and to use the algorithm to “automatically answer the case’s individual questions as to all of the remaining class members—with high accuracy”).

98. Wilf-Townsend, *supra* note 48, at 777.

that aggregation is not just an enforcement vehicle but also a way to create liability rules tailored to group-wide harm. In practice, he urges an “important role” for class actions in AI cases and floats per se or group-based liability regimes that would let a class recover even when no single member can pinpoint an individualized injury.⁹⁹ This proposal may lower the burden of remedy once a pattern is identified, and Wilf-Townsend notes that algorithmic audits or reporting duties could help surface group-level harms that are invisible at the individual level.¹⁰⁰ But those audits and reports lie upstream of litigation and must exist before any class claim can be pleaded. In sum, while Wilf-Townsend makes a plausible case for why invisible algorithmic harms make aggregate litigation compelling, he too leaves the core question unanswered: How, absent proactive oversight, will the facts needed to plead such claims ever come to light?

What emerges from these works is a consensus coupled with a dilemma. Scholars agree that traditional individual litigation is ill suited for the age of invisible algorithms and respond with structural solutions such as tweaking procedural rules, creating new theories of liability, and expanding aggregation mechanisms. But these proposals all require someone to first notice the harm. The detection gap thus remains the upstream bottleneck that no amount of downstream procedural innovation can unclog. Until the law devises better mechanisms for *finding* incognito harms, not just *redressing* them, even the most sophisticated reforms risk addressing only the tip of a submerged iceberg.

2. *Spoliation Doctrine Is a Dead End*

Perhaps the closest existing doctrinal analog to incognito consumer harm’s circumvention of accountability is spoliation, the deliberate destruction of unfavorable evidence. But spoliation doctrine is as much a dead end here as aggregate litigation is, because spoliation sanctions activate only once litigation is pending or reasonably anticipated.¹⁰¹ If evidence disappears *before* anyone foresees a claim, spoliation rules offer no relief.¹⁰² Common law and the Federal Rules of Civil Procedure shield

99. *Id.* at 780, 825.

100. *Id.* at 827.

101. *See, e.g.,* Joshua M. Koppel, *Federal Common Law and the Courts’ Regulation of Pre-Litigation Preservation*, 1 STAN. J. COMPLEX LITIG. 171, 172 (2012) (“The unanimous view of the federal courts is that federal law imposes upon a party a duty to preserve relevant evidence from the time that the party can reasonably anticipate litigation.”).

102. *See, e.g.,* *Turner v. United States*, 736 F.3d 274, 282 (4th Cir. 2013) (denying plaintiff’s spoliation claim because “[w]ithout a warning of future litigation or reason to believe that voice recordings devoid of a rescue call would be relevant in any event, the Coast Guard had no reason to change its standard routine [of periodically destroying voice recordings]”).

parties from sanctions for data lost through routine operations prior to a reasonable anticipation of litigation.¹⁰³ The implication for incognito consumer harm is debilitating: A wrongdoer who keeps victims unaware until the proof is gone can achieve the functional equivalent of spoliation without triggering spoliation doctrine at all.

Worse, modern firms have developed tactics that achieve the functional equivalent of spoliation without triggering any preservation duty, by ensuring that consumers never learn enough to anticipate litigation in the first place. Companies can quietly revise terms or privacy policies to authorize harmful conduct while providing little effective notice. In 2025, for example, Meta introduced an opt-in feature that uploaded private photos, including ones that users had never shared, to its servers for AI processing.¹⁰⁴ Users could turn the feature off, but Meta buried the opt-out in settings and framed it in vague and misleading language.¹⁰⁵ Rather than stating that private photos would be scanned, Meta described the feature as enabling “camera roll cloud processing” to get “creative ideas made for you”¹⁰⁶—a euphemism bearing no resemblance to what Meta actually does. The result is a preservation trap: By keeping most users unaware and structuring “consent” so any later paper trail favors the company, firms can prevent the outcry or lawsuit that would trigger a duty to preserve evidence.

Similar tactics exploit fragile links in notice and consent. Companies sometimes send mandatory disclosures or opt-out notices in formats that seem designed to be missed. For example, firms craft email “notice” to resemble spam, using sender addresses or content likely to be filtered into junk. Courts often treat an unrejected email as effective notice, in part because spam is not returned as undeliverable.¹⁰⁷ The result is technical compliance with practical invisibility: Consumers never see critical terms like arbitration clauses or settlement notices, and major email services auto-delete spam in thirty days,¹⁰⁸ erasing victims’ opportunity to learn of their rights. After its data breach in 2023, 23andMe reportedly emailed customers about a new mandatory arbitration clause and gave only thirty days to opt

103. See, e.g., *id.*; *Bistrrian v. Levi*, 448 F. Supp. 3d 454, 467 (E.D. Pa. 2020) (noting that Federal Rule of Civil Procedure 37(e) “does not apply to information that was lost or destroyed before a duty to preserve it arose”).

104. See Oestreicher, *supra* note 7.

105. See *id.*

106. *Id.*

107. See Kim, *supra* note 69, at 613–35.

108. *Id.* at 616 n.51.

out.¹⁰⁹ If the email landed in spam, as is designed to happen for many,¹¹⁰ victims could unknowingly forfeit their right to sue. This tactic does not destroy evidence in the classical sense. Instead, it preempts litigation by ensuring that victims remain unaware until it becomes too late to act. In such cases, spoliation sanctions, however potent on paper, would be a dead end because the law never even realized that wrongdoing existed to begin with.

Neither scholars nor courts have addressed this problem. For decades, debates over spoliation focused on how often evidence destruction occurs and whether it should give rise to an independent tort, rather than the doctrine's inherent inability to remedy harms designed to prevent litigation from arising in the first place.¹¹¹ By the early 2000s, many scholars were urging the recognition of a standalone spoliation cause of action, reflecting a consensus that existing sanctions were inadequate deterrents.¹¹² Courts, however, have been skeptical of expanding the doctrine.¹¹³ In *Cedars-Sinai Medical Center v. Superior Court*, the California Supreme Court refused to recognize a tort remedy for first-party spoliation, reasoning that the "infrequency of spoliation" suggested that existing remedies were "generally effective" deterrents.¹¹⁴ This reasoning presumes that evidence destruction will likely surface in litigation and be sanctioned accordingly. But it fails to account for a more insidious reality: incognito consumer harm in which perpetrators preempt any chance of litigation, and therefore any duty to preserve evidence, by concealing the injury itself. In such scenarios, the trigger for spoliation doctrine is deliberately never reached, rendering it a dead end for incognito harm.

109. Pranav Dixit, *23andMe Frantically Changed Its Terms of Service to Prevent Hacked Customers from Suing*, ENGADGET (Dec. 8, 2023, at 10:24 ET), <https://www.engadget.com/23andme-frantically-changed-its-terms-of-service-to-prevent-hacked-customers-from-suing-152434306.html> [https://perma.cc/WB4J-HJRP].

110. See Kim, *supra* note 69, at 613–35.

111. See Deborah L. Rhode, *Ethical Perspectives on Legal Practice*, 37 STAN. L. REV. 589, 598–99 (1985) (noting that half of large-firm litigators surveyed deemed evidence disclosure problems "regular or frequent"); Charles R. Nesson, *Incentives to Spoliate Evidence in Civil Litigation: The Need for Vigorous Judicial Action*, 13 CARDOZO L. REV. 793, 793 (1991) (describing how spoliation had become "an effective . . . and . . . growing litigation practice").

112. See, e.g., Chris William Sanchirico, *Evidence Tampering*, 53 DUKE L.J. 1215, 1280 (2004) ("[T]he general position among scholars [is] that [spoliation of evidence tort claims] should be maintainable . . .").

113. See *Trevino v. Ortega*, 969 S.W.2d 950, 952 (Tex. 1998) (declining to recognize a cause of action for spoliation); *id.* at 953 (citing other jurisdictions that declined to recognize separate causes of action for conduct related to spoliation such as perjury or embracery).

114. *Cedars-Sinai Med. Ctr. v. Superior Ct.*, 954 P.2d 511, 520 (Cal. 1998).

3. *Regulatory Proposals: No “Alarm Bell” for Hidden Harms*

Like litigation, U.S. consumer protection enforcement remains largely reactive, hinging on consumers to report wrongdoing. The Consumer Financial Protection Bureau, for instance, “uses complaints to inform supervision and examination, rulemaking, [and] enforcement actions”¹¹⁵ and “has repeatedly stated that it will consider complaints as a basis for deciding who to examine and/or investigate.”¹¹⁶ State attorneys general, too, rely on public complaints, “which often serve[] as the starting point for later enforcement actions.”¹¹⁷ While consumer reports are an indispensable component of enforcement, the flaw is evident: When the harm is invisible, as incognito consumer harm is, consumers report nothing because they do not know that they were harmed. This renders the existing “squeaky wheel” enforcement apparatus ineffective against many newly rising consumer harms, such as behind-the-scenes pricing algorithms, discriminatory targeting, and data handling abuses.

New York’s Algorithmic Pricing Disclosure Act succinctly illustrates the problem. It requires businesses that use personal data to personalize prices to post a conspicuous notice: “THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA.”¹¹⁸ Enforcement rests with the New York Attorney General, who can act on a “reason to believe” that a violation occurred. On the eve of the law’s effective date, the Attorney General even urged New Yorkers to report retailers that fail to comply.¹¹⁹ But consumers have no independent way to know whether their prices were algorithmically personalized. Even if firms omitted the notice, no one would have reason to suspect that a disclosure was required but withheld.¹²⁰ A transparency mandate cannot deter hidden pricing discrimination when

115. Angela Littwin, *Why Process Complaints? Then and Now*, 87 TEMP. L. REV. 895, 895 (2015).

116. Alan S. Kaplinsky, *CFPB Expanded Consumer Complaint Database Raises Concerns*, 67 CONSUMER FIN. L.Q. REP. 189, 189 (2013).

117. Mark Totten, *Credit Reform and the States: The Vital Role of Attorneys General After Dodd-Frank*, 99 IOWA L. REV. 115, 142 (2013).

118. N.Y. GEN. BUS. LAW § 349-a(2) (McKinney 2026).

119. See Press Release, Letitia James, Att’y Gen. of N.Y., Consumer Alert: Attorney General James Warns New Yorkers About Algorithmic Pricing as New Law Takes Effect (Nov. 5, 2025), <https://ag.ny.gov/press-release/2025/attorney-general-james-warns-new-yorkers-about-algorithmic-pricing-new-law-takes-effect> [https://perma.cc/J6H5-Y2KK] (“Attorney General James is encouraging consumers to file complaints . . . if they encounter algorithmic pricing that is not properly disclosed.”).

120. Talia B. Gillis, *“Price Discrimination” Discrimination*, 15 HARV. BUS. L. REV. 99, 133 (2025) (“Firms tend to conceal their pricing policies, particularly when they . . . could cause . . . backlash. As a result, publicly known examples of PD are far fewer than their real-life prevalence.”).

violators can plausibly bet that almost no one will detect the underlying practice.

New York is not alone in enacting disclosure laws that, in practice, amount to self-policing and are easily gamed when no one is watching. Illinois's Artificial Intelligence Video Interview Act of 2019, praised in the literature as a model for other states,¹²¹ requires employers using AI-driven video interviews to notify applicants that AI will be used, explain how it works, obtain consent, and limit sharing and retention of recordings.¹²² If an employer relies solely on AI analysis of video interviews to select applicants for in-person interviews, the Act also requires it to collect and annually report demographic data for state analysis of disparate impact.¹²³ Similarly, Maryland enacted a law requiring employers to obtain applicants' written consent before using facial recognition technology in job interviews.¹²⁴ In theory, these disclosure and self-reporting obligations should expose AI bias and protect job applicants from hidden discrimination.

In practice, these regimes will likely be just as ineffective at deterring hidden harms. The Illinois law's reporting requirement can be evaded by inserting a token human reviewer into the hiring process so that the employer can claim not to rely "solely" on AI. Employers in Maryland or Illinois can simply refuse to provide the required notice to candidates, betting that a rejected applicant would not know that an algorithm or facial recognition was involved and thus would not complain. Crucially, Illinois's law lacks any robust detection or oversight mechanism for unreported violations. Compliance is effectively self-reported because employers supply the required data, and the law does not authorize regulators to independently collect or verify it.¹²⁵ The same disjunction between aspiration and enforcement plagues other domains. Many online age-verification laws enacted since 2020 require platforms to collect a user's ID for age checks and then purge the sensitive data immediately to prevent misuse. But without audits, enforcement relies entirely on consumers

121. Sonia M. Gipson Rankin, *The MiDAS Touch: Atuahene's "Stategraft" and Unregulated Artificial Intelligence*, 98 N.Y.U. L. REV. ONLINE 225, 244 (2023) ("The White House's Blueprint for AI Bill of Rights is a good step towards addressing the impact of AI Seventeen states introduced general artificial intelligence bills . . . in 2022"); *id.* at 244 n.107 (referencing Illinois's Artificial Intelligence Video Interview Act); Brittany Kammerer, Note, *Hired by a Robot: The Legal Implications of Artificial Intelligence Video Interviews and Advocating for Greater Protection of Job Applicants*, 107 IOWA L. REV. 817, 836 (2022) (arguing that Illinois's Artificial Intelligence Video Interview Act is a "good template for other . . . states").

122. 820 ILL. COMP. STAT. ANN. 42/5, 42/10, 42/15 (West 2026).

123. 820 ILL. COMP. STAT. ANN. 42/20 (West 2026).

124. MD. CODE ANN., LAB. & EMPL. § 3-717 (West 2026).

125. 820 ILL. COMP. STAT. ANN. 42/20 (West 2026) (requiring employers to collect and report limited demographic data and the relevant state authority to analyze the reported data).

“trust[ing] that companies will actually delete” their data as promised, a premise which a federal court called “dubious.”¹²⁶ In each case, a disclosure-based law which assumes that transparency without oversight can cure algorithmic harms would end up with neither transparency nor cure.

The detection gap is not merely a problem of legislative design. It persists in the scholarly proposals that aim to fix these regimes. Professor Mark Lemley urges the FTC to use its broad authority more aggressively across privacy, consumer protection, and competition to curb “corporate abuse of notice and consent” that leaves consumers unknowingly exposed.¹²⁷ Lemley’s proposal is pragmatic in an important respect, in that he urges regulators to reinterpret their existing statutory remit rather than waiting for unlikely new legislation.¹²⁸ But his argument illustrates a recurring pattern across existing literature: Even when scholars correctly diagnose the problem—that notice and consent in the consumer economy have become fictitious—they prescribe solutions that still depend on someone detecting the violation. A company can quietly harvest data or slip onerous clauses into fine print, and, absent a whistleblower, audit, or investigative exposure, regulators may never learn of the violation. Without mechanisms to uncover hidden violations, even an emboldened FTC would be a watchman waiting for an alarm that never sounds.

Other scholars would impose proactive duties on businesses to prevent hidden harms before they occur. Professors Neil Richards and Woodrow Hartzog, for example, argue that companies entrusted with consumer data should owe a fiduciary duty to “refrain from self-dealing,”¹²⁹ which would prohibit designs that “unreasonably exploit[] our cognitive limitations, biases, and predictable errors.”¹³⁰ A social media platform, for instance, could breach the duty by secretly manipulating a user’s feed in ways that harm the user to increase engagement.¹³¹ Richards and Hartzog propose that a breach of this fiduciary duty “would be a *per se* legal injury” that satisfies the harm requirement for legal action.¹³² While the legal standard itself is

126. *Free Speech Coal., Inc. v. Colmenero*, 689 F. Supp. 3d 373, 400 (W.D. Tex. 2023), *aff’d in part, vacated in part sub nom. Free Speech Coal., Inc. v. Paxton*, 95 F.4th 263 (5th Cir. 2024), *aff’d*, 606 U.S. 461 (2025).

127. Lemley, *supra* note 11, at 248.

128. *Id.* at 258–59 (arguing the FTC should “expand its authority” over privacy practices and “refuse to enforce” pseudo-contracts because it falls “well within its authority to regulate deceptive acts”).

129. Richards & Hartzog, *supra* note 14, at 964.

130. *Id.* at 1011.

131. *See id.* at 1004 (“Informational capitalism demands your personal data and your attention. Consequently, companies do everything . . . to make you feel safe to expose yourself online.”).

132. *Id.* at 1012.

well conceived, Richards and Hartzog provide no practical mechanism to monitor a company's opaque decisionmaking. A design choice that quietly benefits the company at the expense of consumers can violate the duty long before any outsider notices.

Professor Lauren Willis advances "performance-based" consumer protection rules that set outcome-based standards and have regulators monitor real-world results. For example, a rule might require that "at least 80 percent of consumers who are paying a given fee know the existence and amount of the fee,"¹³³ and regulators would survey customers to test their understanding.¹³⁴ While this approach is more empirically grounded, it works best for things that can be openly tested, such as whether consumers understand fee structures. When a harmful practice is hidden—such as a robot vacuum recording video without notice¹³⁵—there is nothing to test because consumers cannot understand what they do not know exists. A firm could satisfy every benchmark for disclosed practices while committing a separate concealed abuse that falls outside any predefined performance metric. Indeed, the fact that DJI Romo robot vacuums recorded video inside consumers' homes was revealed only because the hacker who accidentally gained control of 7,000 devices chose to alert a reporter rather than exploit the access.¹³⁶ Performance-based standards have no metric for misconduct that surfaces only through the goodwill of strangers.

Proposed reform by legislators and regulators also neglects the detection gap. The Algorithmic Accountability Act of 2025, a proposed bill, would require companies to assess and report risks of certain automated decision systems before deployment.¹³⁷ For example, companies would be required to conduct a bias audit of a hiring algorithm and submit results to the FTC.¹³⁸ The FTC's "Junk Fees" rule, which took effect in May 2025, prohibits "drip pricing" by requiring mandatory fees to be disclosed upfront in the total price,¹³⁹ targeting a classic ambush tactic in which consumers learn of charges only at checkout or after purchase. These measures represent a shift to a detection-first design, intended to catch discriminatory or unsafe systems early rather than after they have quietly harmed thousands of people. But they, too, ultimately turn on detection: Reports are useful only

133. Willis, *supra* note 47, at 1312.

134. *Id.*

135. See *The Accidental Hacker: How One Man Gained Control of 7,000 Robots*, *supra* note 4.

136. *Id.*

137. Algorithmic Accountability Act of 2025, S. 2164, 119th Cong. § 3(b)(1)(A) (2025).

138. See *id.* § 3(b)(1)(D).

139. See 16 C.F.R. § 464.3 (2026) ("In any offer, display, or advertisement for a covered good or service it is . . . a violation of this part for any business to misrepresent any fee or charge, including: the nature, purpose, amount, or refundability of any fee or charge . . ."); see also *id.* § 464.2 (requiring disclosure of good or service's "total price").

if someone reviews them and verifies accuracy, and pricing disclosure mandates work only if violations are exposed and pursued.

In sum, these proposals represent a necessary evolution toward prevention, shifting the focus from after-the-fact remedies to before-the-fact precautions. Yet even these forward-looking proposals risk addressing only the harms that announce themselves, while missing the vast swath of incognito injuries that by design fly under the radar. The lesson is subtler and more disquieting than the corresponding lesson from litigation. Litigation's dependence on detection is at least transparent because everyone understands that a plaintiff must know enough to sue. But regulation's dependence on detection is hidden behind the language of proactivity and oversight. A disclosure mandate that no one verifies, an impact assessment that no one audits, and a performance standard that cannot measure what is concealed are proactive in form only. Until the law devises ways to expose the harms that no one is looking for, not just those that regulators already know to look for, even the most well-intended reforms will be incomplete.

B. Hidden Injuries Are Not Legally Recognized as "Harm"

Section A described the first of the twin failures of incognito consumer harm: the law's inability to surface injuries engineered to remain hidden. But the second failure is, in some ways, more perverse than the first. Despite intentional concealment, incognito consumer harm sometimes does come to light, whether through a hack, a whistleblower, or sheer accident.¹⁴⁰ One would expect that once concealment is punctured, the legal system could take over. Yet even then, plaintiffs face an uphill battle convincing courts that a "real" injury occurred because modern doctrine remains wedded to a narrow notion of harm that often excludes the very injuries that hidden schemes inflict. A victim must first beat the long odds to discover the harm, only to be told that what was discovered does not legally count. Three doctrinal hurdles conspire to produce this result: constitutional standing, pleading standards, and class certification requirements. And their practical effect is uniform: The more successfully a firm keeps its misconduct internal—avoiding third-party disclosure, preventing downstream misuse, and leaving no externally observable trace—the less likely courts are to treat the resulting injury as legally actionable.

Article III standing requires a plaintiff to show an "injury in fact," an invasion of a legally protected interest, that is "concrete, particularized, and

140. See *supra* notes 1, 4–5 and accompanying discussion.

actual or imminent.”¹⁴¹ For claims resting on a defamation analogy, constitutional standing may turn on whether the information at issue was “published to a third party.”¹⁴² In *TransUnion LLC v. Ramirez*, a credit reporting company had falsely flagged thousands of consumers as potential terrorists.¹⁴³ The Supreme Court held that only the 1,853 plaintiffs whose false reports were disclosed to third parties had standing, while the remaining 6,332 lacked a “concrete” injury.¹⁴⁴ Although the parties assumed that TransUnion had violated the relevant statute even without third-party publication,¹⁴⁵ the Court reasoned that “an asserted *risk of future harm*” was insufficient and third-party publication was a “longstanding” common-law requirement.¹⁴⁶ Justice Thomas’s dissent argued that the majority had “relieved the legislature of its power to create and define rights.”¹⁴⁷ This Article’s analysis supports that concern but identifies an additional dimension the dissent did not address: The majority’s framework creates a feedback loop in which firms that invest in concealment receive a standing windfall, because the injuries they inflict are the ones least likely to satisfy the Supreme Court’s test for concreteness.¹⁴⁸

TransUnion recognizes intrusion as a concrete injury, yet endorses an approach to unauthorized retention that is difficult to reconcile with the common law’s own privacy torts. Intrusion upon seclusion, for example, protects against the invasion itself—the act of intruding into a person’s private affairs—regardless of whether the intruder ever discloses what was found to anyone else. No publication is required because the wrong is complete upon the intrusion.¹⁴⁹ *TransUnion* approvingly cited *Braitberg*,

141. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021).

142. *Id.* at 432.

143. *Id.* at 419–20.

144. *Id.* at 433.

145. 15 U.S.C. § 1681e(b) (accuracy requirement); *id.* § 1681n(a) (“Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer . . .”). See *TransUnion*, 594 U.S. at 432 n.5 (noting the parties’ assumption of a statutory violation despite nondissemination and expressly declining to decide that issue).

146. *TransUnion*, 594 U.S. at 432, 435–37.

147. *Id.* at 454 (Thomas, J., dissenting).

148. The perversity extends beyond concealment. In some data breach cases, courts have denied standing to plaintiffs who canceled compromised credit cards—reasoning in part that the cancellations eliminated the risk of future credit card fraud. The result is that diligent consumers are punished for precisely the kind of protective action the law should encourage: The more effectively a victim mitigates, the less likely a court is to find standing. See, e.g., *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344–45 (11th Cir. 2021) (explaining how plaintiff’s cancellation of compromised cards “effectively eliminat[ed] the risk of credit card fraud”); *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89, 90–91 (2d Cir. 2017) (finding no standing where compromised credit card was promptly canceled and no other personal information was stolen).

149. See RESTATEMENT (SECOND) OF TORTS § 652B (A.L.I. 1977); *id.* cmt. a (“The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person

which rejected standing for retaining information initially obtained lawfully beyond a statutory destruction deadline where no further use, disclosure, or material risk of harm was alleged.¹⁵⁰ Applied to a company retaining intimate photos it promised to delete, that reasoning understates the privacy invasion inherent in continued possession of information the company no longer has permission to keep.

This approach means that, even if incognito consumer harms are eventually exposed, courts may still treat them as non-cognizable. Consider slight variations on real privacy harms. In 2023, the FTC sued the Amazon-owned firm Ring for allowing an employee to view “thousands of video recordings belonging to at least 81 unique female users” that “surveilled an intimate space, such as ‘Master Bedroom,’” and for allowing “hundreds of employees and Ukraine-based third-party contractors . . . access to all video data.”¹⁵¹ The dating advice app Tea collected photo IDs and selfies for verification and promised to delete them, but retained them for years until a hack exposed the data.¹⁵² Now assume that Ring and Tea initially obtained the videos and IDs with valid consent but retained them in secret after the promised deletion date, without further use or third-party access. Further imagine that whistleblowers in both companies come forward so that the victims learn of the harm. In these hypotheticals, there is a clear invasion of privacy—companies retained intimate data they promised to delete—but a court following *Braitberg*’s approach could require a further showing of concrete injury. The conduct could still support FTC enforcement for deceptive omission under Section 5(a) of the FTC Act, but even successful privacy enforcement can yield only modest recoveries.¹⁵³

Scholars have criticized courts for “adopting a particular perspective on the nature and value of privacy” and “shifting” standing law to dismiss claims based on “[judicial] views on the nature and value of the asserted

whose interest is invaded or to his affairs.”); *id.* cmt. b (“The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.”).

150. *TransUnion*, 594 U.S. at 425, 434 (citing *Braitberg v. Charter Commc’ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016)).

151. Complaint at 6–7, *FTC v. Ring LLC*, No. 1:23-cv-01549 (D.D.C. May 31, 2023).

152. See Kwai, *supra* note 5.

153. Cf. Peter Ormerod, *Privacy Qui Tam*, 98 NOTRE DAME L. REV. 267, 270 (2022) (“[E]ven successful [privacy enforcement] actions have extracted disappointing penalties and underwhelming concessions.”); Diane Bartz, *Amazon’s Ring Used to Spy on Customers, FTC Says in Privacy Settlement*, REUTERS (May 31, 2023, at 19:57 ET), <https://www.reuters.com/legal/us-ftc-sues-amazoncoms-ring-2023-05-31/> [<https://perma.cc/22L3-8WMK>] (noting that Amazon settled for \$5.8 million in the Ring case with the FTC).

harms.”¹⁵⁴ But the problem extends beyond the narrowness of the privacy harms that courts recognize. More fundamentally, victims, courts, and even companies themselves often do not know whether disclosure occurred. This is because “hackers have an incentive to commit breaches without being detected” so they can continue breaching undetected,¹⁵⁵ a lesson familiar since at least World War II.¹⁵⁶ Incognito consumer harm exploits this uncertainty by both hiding wrongdoing and obscuring whether the “publication” that standing doctrine often requires actually happened. Yet, broadening the range of cognizable injuries does not itself reveal whether those injuries occurred. Standing doctrine can thus impose an impossibly high bar for privacy plaintiffs, rewarding defendants whose concealment makes the necessary facts unknowable.

Judicial skepticism of privacy, data, or algorithmic injuries is only the beginning. Courts often recognize modern injuries only when those injuries pretend to be old ones—treating continued possession of lawfully obtained information as harmless in itself, for example, even after the company is legally required to destroy it. A concealed data practice becomes legible if it resembles publication, reputational injury, fraud, or trespass; it becomes legally suspect when the injury instead consists of engineered ignorance, loss of control, or deprivation of the information needed to object, exit, or sue. Incognito consumer harms should not be treated as benign versions of old torts. They are wrongs that the legal system has not yet built adequate categories for, and forcing them into inherited templates only obscures the injury. One aim of the reforms proposed in Part III is to help courts and regulators recognize modern injuries without forcing them into analogies that erase what makes them modern.

Twombly and *Iqbal*’s plausibility standard creates a second filter that disproportionately screens out incognito harm.¹⁵⁷ The well-known post-*Iqbal* catch-22 is that plaintiffs need discovery to plead plausibly but cannot get discovery without first pleading plausibly.¹⁵⁸ Incognito harm intensifies

154. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 450 (2017); see also Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. REV. ONLINE 62, 62–64 (2021); Summer Elliot, Note, *There’s No Understanding Standing for Privacy: An Analysis of TransUnion v. Ramirez*, 37 BERKELEY TECH. L.J. 1379, 1380 (2022).

155. Yunsieq P. Kim, *Redefining “No Evidence of a Breach” in Election Security*, 76 SMU L. REV. F. 130, 137 (2023).

156. *Id.* at 139.

157. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556–58 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678–80 (2009).

158. See, e.g., Arthur R. Miller, *From Conley to Twombly to Iqbal: A Double Play on the Federal Rules of Civil Procedure*, 60 DUKE L.J. 1, 20 (2010) (arguing that plausibility pleading “is a form of fact pleading by another name”).

this problem because concealment withholds the very kinds of facts that courts treat as indicia of real-world injury. This is particularly true in modern privacy and technology disputes, where plausibility pleading too often tends to privilege injuries with externally legible footprints: disclosure to third parties, concrete downstream misuse, measurable financial loss, or other observable consequences. When information asymmetry is strategic, as in when a product is designed so that outsiders cannot observe how it operates, pleading doctrine becomes a substantive sorting mechanism. Injuries that leave no outward trace are treated as conjectural; injuries that happen to surface look “real” enough to plead.¹⁵⁹ Plausibility doctrine thus rewards successful concealment by converting non-observability into non-cognizability.¹⁶⁰

Proposals to ameliorate this catch-22 without enabling so-called “fishing expeditions” often take the form of limited pre-suit discovery in asymmetric information cases.¹⁶¹ Other works argue that courts should credit “institutional” facts, such as agency investigations, technical audits, or other competent determinations, as a basis for plausibility where defendants control the relevant evidence.¹⁶² For incognito consumer harm, the lesson is that pleading rules cannot be treated as a neutral screen. If legal cognizability is defined by what can be pled with outward-facing detail, the injuries most likely to go unseen will predictably be the injuries that the law declines to recognize.

Finally, incognito consumer harm collides with class action doctrine in a way that approaches paradox. Class actions are defended as the procedural device best suited to address low-value, widespread consumer wrongdoing.¹⁶³ After *TransUnion*, however, a damages class cannot meaningfully remedy hidden injuries if many class members are deemed “uninjured” under Article III’s narrow conception of cognizable harm. The

159. See, e.g., Sam Gilman, Note, *Proliferating Predation: Reverse Redlining, the Digital Proliferation of Inferior Social Welfare Products, and How to Stop It*, 56 HARV. C.R.-C.L. L. REV. 169, 220 (2021) (noting that in algorithmic advertising discrimination cases, the defendant platform or advertiser may “have sole access to the data needed to credibly allege the discriminatory practice,” making it implausible for plaintiffs to plead such hidden biases without discovery).

160. See, e.g., Christopher R. Leslie, *How to Hide a Price-Fixing Conspiracy: Denial, Deception, and Destruction of Evidence*, 2021 U. ILL. L. REV. 1199, 1202, 1238–42 (explaining that plausibility pleading “reward[s] the various concealment methods” used by conspirators, leading judges to dismiss claims that lack details that conspirators have successfully hidden). Although Leslie addresses antitrust concealment, the dynamic applies with equal force to incognito consumer harm, where the product itself is designed to prevent observation. See *id.*

161. See, e.g., Fabio Arcila, Jr., *Plausibility Pleading as Misprescription*, 80 BROOK. L. REV. 1487, 1527 (2015).

162. See, e.g., Benjamin Shand, Note, *Institutional Facts: Responding to Twombly and Iqbal in the District Courts*, 98 N.Y.U. L. REV. 1446, 1457 (2023).

163. See, e.g., Miller, *supra* note 12; Salib, *supra* note 94; Wilf-Townsend, *supra* note 48, at 797.

Court held that “every class member must have Article III standing in order to recover individual damages.”¹⁶⁴ That requirement is virtually a gift for incognito harm, because concealment often ensures that many victims cannot show the kind of concrete injury that existing doctrine demands—especially when the claim depends on third-party disclosure or realized monetary loss.¹⁶⁵ The more successfully a scheme keeps harm internal, ambiguous, or undisclosed, the more likely it is to produce a damages class that is either entirely uncertifiable or drastically underinclusive.

The Supreme Court has so far avoided clarifying when, exactly, absent class members must demonstrate standing. *TransUnion* reserved the question,¹⁶⁶ and the Court’s dismissal of *Labcorp v. Davis* as improvidently granted left it unresolved.¹⁶⁷ The practical consequence of this doctrinal uncertainty is predictable: Defendants can leverage standing to fracture proposed classes and demand individualized showings that are impossible when the injury’s very existence is concealed. Class actions are supposed to expose and deter systematic misconduct,¹⁶⁸ but modern standing doctrine makes class-wide relief hardest where wrongdoing is the most successfully hidden.

Taken together, standing, pleading, and certification filter consumer harm through visibility: An injury without an observable footprint can become an injury without a remedy. Section A showed that incognito harms are difficult to detect. This Section has shown that detection does not guarantee recognition. Even when misconduct comes to light, claims may still be screened out by doctrines calibrated to public manifestation, detailed factual access, individualized proof, or measurable loss. The result is a sequential distortion: The legal system first underdetects hidden harm and then underrecognizes the hidden harm that it manages to detect. Section C explains why these two failures produce a systematically distorted picture of legally cognizable consumer injury.

164. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021).

165. *See supra* Section II.B.

166. *TransUnion*, 594 U.S. at 431 n.4.

167. *Lab’y Corp. of Am. Holdings v. Davis*, 605 U.S. 327, 327 (2025) (“The writ of certiorari is dismissed as improvidently granted.”); *id.* at 328 (Kavanaugh, J., dissenting) (“The Court dismisses the case as improvidently granted and therefore does not decide the question presented: Whether a federal court may certify a damages class pursuant to Federal Rule of Civil Procedure 23 when the class includes both injured and uninjured class members.”).

168. *See, e.g., Miller, supra* note 12; Salib, *supra* note 94; Wilf-Townsend, *supra* note 48.

C. Survivorship Bias Distorts the Law's Perspective of Consumer Harm

During World War II, the U.S. military examined aircraft returning from combat and mapped where the surviving planes were damaged. Officers with “vast[] . . . knowledge and understanding of aerial combat” concluded that the parts with the most bullet holes—the wings and fuselage—should be reinforced with armor.¹⁶⁹ But a young statistician named Abraham Wald saw the flaw in this logic: The data came only from the planes that survived. The parts that needed armor were those where the returning planes had the *least* damage—the engine and cockpit—because the planes struck there apparently never made it back.¹⁷⁰ For all their expertise, the officers were reasoning from a biased sample: They saw only the subset that survived a filter and mistook that subset for the whole.

Incognito consumer harm exposes the same epistemic trap in law. Sections A and B identified two sequential filters that screen out hidden harms: detection and legal cognizability. Beyond creating disjunctions in enforcement, these filters systematically distort the legal system’s working picture of what “consumer harm” looks like.

The law’s picture of consumer harm is not drawn from a neutral census of injuries. It is drawn from the subset of injuries that become visible enough to trigger enforcement and then survive the system’s screening rules. Detection filters out what is never noticed, and cognizability filters out what is noticed but existing doctrine cannot narrate as injury. What remains—harms conspicuous enough to generate a complaint and legible enough to satisfy standing, pleading, and certification—is mistaken for the full universe of consumer injury. Courts form intuitions about what “real” harm looks like from the cases that reach them. Agencies infer what problems “exist” from the complaints they receive. Scholars build diagnoses from litigated disputes. Each step is rational in isolation, but the record is a biased sample because incognito harms are disproportionately filtered out before they ever become data.

This helps explain a recurring pattern in the literature. Scholars have produced vibrant work on how corporations defeat claims through mandatory arbitration,¹⁷¹ how mass arbitration emerged as a counter-strategy,¹⁷² and how firms have modified arbitration clauses to deter mass

169. JORDAN ELLENBERG, *HOW NOT TO BE WRONG: THE POWER OF MATHEMATICAL THINKING* 13–14 (2014).

170. *Id.* at 13.

171. David Horton, *Infinite Arbitration Clauses*, 168 U. PA. L. REV. 633, 633 (2020).

172. J. Maria Glover, *Mass Arbitration*, 74 STAN. L. REV. 1283, 1288–89 (2022).

filing.¹⁷³ While those tools are consequential, they are downstream of a far more decisive act in the case of incognito consumer harm: A firm that keeps its practice invisible forecloses the very possibility of a claim ever being filed. Invisibility functions as a pre-pleading, pre-standing, and pre-class action liability shield.

Survivorship bias distorts not only what the law sees, but also who it suspects. Conventional accounts treat large repeat-player companies as the primary perpetrators of consumer-facing wrongdoing because larger firms have the resources for costly litigation¹⁷⁴ and the scale to reap large profits from misconduct.¹⁷⁵ This narrative explains which firms are more likely to commit *conspicuous* harms, where a wrongdoer's sole refuge once a claim is filed is to resist liability via procedural obstruction, such as forum shopping. But the narrative is unlikely to hold for incognito harm. Assume that one consumer in a thousand detects an incognito harm and one in a thousand who detects it actually sues, thus yielding one claim per million harmed consumers. A firm with a million customers would expect a single complaint, while a firm with ten thousand could expect none. Holding per-customer gain constant, the smaller firm's expected liability is lower because its victim pool is too small to produce even one visible case. In other words, although large firms are hardly innocent, "repeat-player" status is an incomplete predictor of who would commit incognito harm. The strategy is most attractive where the victim pool is small, fragmented, or transient, and where reputational feedback is weak.

This difference also affects deterrence. For conspicuous harms, the severity of punishment is roughly proportional to the degree of deterrence because, at least in theory, punishment can be reasonably expected for anyone who commits harm. For incognito harm, the expected cost of misconduct depends both on the severity of the punishment *and* on the

173. Richard Frankel, *Fighting Mass Arbitration: An Empirical Study of the Corporate Response to Mass Arbitration and Its Implications for the Federal Arbitration Act*, 78 VAND. L. REV. 133, 133 (2025).

174. Rachel H. Yarkon, Note, *Bargaining in the Shadow of the Lawyers: Negotiated Settlement of Gender Discrimination Claims Arising from Termination of Employment*, 2 HARV. NEGOT. L. REV. 165, 189 n.119 (1997) ("Smaller companies are likely to be more risk averse than larger companies that have relatively less at stake in an individual case."); Erin A. O'Hara, Note, *Hedonic Damages for Wrongful Death: Are Tortfeasors Getting Away with Murder?*, 78 GEO. L.J. 1687, 1690 n.13 (1990) ("[A] potential tortfeasor [who] is risk averse . . . will be willing to spend more time and money taking care than is efficient because the possibility of large litigation and liability costs presents an additional source of discomfort . . .").

175. Cf. Dorothy S. Lund & Natasha Sarin, *Corporate Crime and Punishment: An Empirical Study*, 100 TEX. L. REV. 285, 341 (2021) ("[F]or the largest firms, even sky-high penalties are likely viewed as just another cost of doing business . . .").

probability of getting caught.¹⁷⁶ When detection probability approaches zero, even the most severe remedies can become largely irrelevant. Research on deterrence consistently finds that *certainty* of punishment suppresses offending more effectively than *severity*, in part because actors cognitively discount penalties they perceive as unlikely to materialize.¹⁷⁷ A related but distinct consideration is the *speed* of enforcement response. Deterrence theorists have long identified celerity (the swiftness of punishment) as a third dimension of the deterrence calculus alongside certainty and severity.¹⁷⁸ In the incognito consumer harm context, delayed enforcement does more than weaken deterrence by compounding the underlying injury. Data collected in violation can be further shared, sold, or breached with each passing day; algorithmic harms can accumulate across millions of transactions; and the evidentiary trail can degrade as systems are updated and logs are overwritten. Timely enforcement is therefore a harm-reduction imperative, beyond its function in deterrence. The intuitive response, simply raising sanctions to offset low detection, thus fails on its own behavioral terms: A penalty that a rational actor never expects to face does not enter the calculus, no matter how large it is on paper. Moreover, when detection depends on breaches, leaks, and whistleblowers rather than systematic oversight, enforcement becomes both weak and, worse, *arbitrary*—punishing the unlucky rather than the culpable and leaving identically situated wrongdoers untouched based on fortuity rather than fault.

Survivorship bias also distorts assumptions about the *type* of harm. The familiar kind is diffuse harm: small losses spread across many, rationally ignored by individual victims, and therefore requiring aggregation. A typical example is a hidden monthly fee of 61 cents that AT&T charged millions of consumers and escalated to \$1.99 before a class action was brought.¹⁷⁹ But diffuse harm is only the visible subset. AT&T likely calibrated the fee to suppress the likelihood that anyone would deem it worth litigating. When the injury is unseen, this constraint relaxes. A firm

176. See, e.g., Nuno Garoupa, *Optimal Magnitude and Probability of Fines*, 45 EUR. ECON. REV. 1765, 1766 (2001) (citing Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968)) (“When deciding whether . . . to commit an act, an individual compares the benefit from the act with the expected punishment. The expected punishment is given by the probability of detection and punishment times a monetary sanction.”).

177. See, e.g., Daniel S. Nagin, *Deterrence in the Twenty-First Century*, 42 CRIME & JUST. 199, 199 (2013) (finding stronger support for increasing the perceived likelihood of apprehension than severity of punishment).

178. See, e.g., Raymond Paternoster, *How Much Do We Really Know About Criminal Deterrence?*, 100 J. CRIM. L. & CRIMINOLOGY 765, 782–84 (2010) (discussing certainty, severity, and celerity as core deterrence variables).

179. Brodtkin, *supra* note 37.

can impose substantial per-capita injury—extracting sensitive data, shifting risk, or silently degrading quality—without provoking resistance, precisely because consumers do not know what was taken. Incognito harm thus undermines two central assumptions that structure reform debates: that corporate wrongdoing will be committed chiefly by large repeat players and designed chiefly to be small and diffuse.

The survivorship bias problem is apparent in otherwise careful empirical scholarship. Professor Charlotte Tschider’s empirical study of data breach litigation analyzes 225 data breach cases from 2005 to 2022 and frames the project in part as a test of common perceptions about breach litigation, including Article III standing challenges that have been “a nearly insurmountable obstacle.”¹⁸⁰ That framing both is accurate *and* shows why the dataset suffers from a survivorship bias. A study of *litigated* breach cases necessarily excludes undetected breaches, incidents detected but not attributable, and injuries for which claims are never filed because courts refuse to treat them as cognizable absent outward-facing indicia such as downstream misuse. The limitation is structural rather than methodological: The study tells us what courts do *once a breach becomes a case*. It cannot see the larger universe of harms that never survive the detection and cognizability filters. If scholars take the docket as the full universe of consumer injuries, they risk treating the “typical” privacy harm as the one that produces a filed case and the “typical” obstacle as the one courts confront after suit, while the more basic question of how many harms never reach court remains systematically off-docket and off-theory.

The literature’s existing tools are not misguided in their own domains. Arbitration reform, class action doctrine, and aggregation mechanisms are necessary responses to conspicuous harm. But those solutions are designed for the harms that survive the system’s filters. Put differently, existing solutions are for the planes that returned, but incognito consumer harm is the plane that did not. The implication for Part III is therefore architectural: The law must build upstream detection capacity that generates cases in the first place and must treat concealment itself as the kind of wrong that the system is designed to catch.

III. REFORMING THE SYSTEM: FROM DETECTION TO ENFORCEMENT

Part II’s diagnosis has a simple implication: No enforcement regime can deter, compensate, or even identify a harm that it does not reliably detect. Incognito consumer harm collapses the ordinary probability of detection at

180. Charlotte A. Tschider, *Unto the (Data) Breach*, 59 U. RICH. L. REV. 591, 591 (2025).

the system's front end, making familiar proposed reforms—tougher penalties, broader standing, looser certification—downstream repairs to a system that fails upstream.

Granted, incremental reform within existing legal frameworks can help. Certain standing failures, for example, can sometimes be mitigated by reframing a hidden data practice as a benefit-of-the-bargain deception. If a company promises to delete customers' personal information after identity verification but secretly retains the data, the plaintiffs could bring a fraud claim (under the reasoning that they would not have used the company's service had they known) rather than a nebulous "data handling" injury.¹⁸¹ But such measures presuppose that concealment has already been punctured by an accident, hack, or whistleblower. For a phenomenon defined by invisibility, the legal system cannot treat discovery as an accidental prerequisite. Meaningful reform must build discovery into the system's design. It must also free courts from having to recognize modern injuries only by analogy to historical torts that were never designed for them—a structural limitation that detection-first reform helps overcome by generating the evidence, and ultimately the doctrinal vocabulary, that inherited categories lack.

Part III therefore shifts the center of gravity from ex post remedies to ex ante revelation by treating detection as a coequal pillar of consumer protection, alongside deterrence and compensation.¹⁸² When wrongdoers profit by keeping conduct invisible, reforms that work only after a complaint is filed are structurally underinclusive. What is needed is a regime that makes concealment harder to maintain, more likely to be discovered, and far more costly once exposed.

A. Beyond Tweaks: Embracing a Detection-First Paradigm

Political scientists have long distinguished between two models of regulatory oversight called "police patrol" and "fire alarm."¹⁸³ Police patrol

181. See, e.g., *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 910 (8th Cir. 2016) ("[Plaintiff's] allegation that he did not receive the data protection set forth in GameStop's policies suffices to support standing to assert claims related to GameStop's unjust retention of his payment."); *Dinerstein v. Google, LLC*, 73 F.4th 502, 517–18 (7th Cir. 2023) (distinguishing the case at bar from *Carlsen* without rejecting the benefit-of-the-bargain theory accepted by the Eighth Circuit).

182. This Article focuses on civil enforcement. Criminal liability for incognito consumer harm raises distinct questions—including the appropriate mens rea standard, the application of respondeat superior to corporate defendants, and the allocation of prosecutorial resources—that warrant separate treatment. The detection-first reforms proposed here would generate information useful to criminal enforcers as well, but the design of criminal sanctions is beyond this Article's scope.

183. See Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 166 (1984).

oversight involves regulators directly monitoring compliance by, for example, inspections, audits, and required reporting. Fire alarm oversight relies on third parties, often victims, to detect and report violations. The choice between the two models depends on whether the alarm is likely to sound. When it can sound because harms are visible and reporting channels function, fire alarm oversight is efficient. When it cannot sound because the harm is invisible, relying on fire alarms is closer to hope than oversight.

Consumer protection for privacy and digital markets still relies heavily on the fire alarm model. Part II showed why that approach fails for incognito consumer harm: Victims do not complain when they do not know that they were harmed and, even when harms surface by accident, doctrine often refuses to recognize them. The question is whether a detection-first alternative—police patrol oversight for consumer technology—is feasible. I argue that it is, as it exists in other domains. This Article’s detection-first approach builds on the insight that consumer protection may require monitoring and supervision beyond ex post enforcement, while shifting the focus to a narrower problem: systems designed, structured, or allowed to prevent the ordinary triggers of enforcement from firing.¹⁸⁴ Detection-first oversight is how the law already governs risks that are too catastrophic, technical, or opaque to leave to victim awareness. In high-risk sectors, regulators routinely inspect, monitor, and audit, because the alternative is to learn about violations from victims only after catastrophe. The Nuclear Regulatory Commission’s oversight is inspection-heavy by design, with about 1,000 safety inspections annually across fuel, reactor, and materials licensees.¹⁸⁵ Its specialists conduct routine inspections at each operating plant because safety risks do not self-report until after failure.¹⁸⁶ The same logic animates environmental monitoring. Environmental law relies on mandated measurement rather than complaints because pollution harms are often invisible at the point of exposure. The EPA requires continuous emission monitoring in certain contexts to catch violations that would otherwise stay undetected.¹⁸⁷

184. See, e.g., Van Loo, *supra* note 16, at 1578; Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1312 (2015).

185. *NRC at a Glance*, NUCLEAR REGUL. COMM’N (Feb. 2, 2026), <https://www.nrc.gov/about-nrc/nrcataglance> [<https://perma.cc/7K25-MUZY>].

186. *Backgrounder on Oversight of Nuclear Power Plants*, NUCLEAR REGUL. COMM’N (Jan. 6, 2021), <https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/oversight> [<https://perma.cc/434L-4AUH>] (describing routine inspections conducted each year at each nuclear power plant).

187. *EMC: Continuous Emission Monitoring Systems*, EPA (Feb. 23, 2026), <https://www.epa.gov/emc/emc-continuous-emission-monitoring-systems> [<https://perma.cc/KAV4-MM2E>] (“CEMS are required under some of the EPA regulations for either continual compliance determinations or determination of exceedances”); 40 C.F.R. § 60.7 (2025) (recordkeeping and reporting requirements).

Other regimes use the same template. The FDA conducts inspections to protect consumers from unsafe products.¹⁸⁸ The Federal Aviation Administration's safety oversight of airlines is explicitly organized around certification and surveillance rather than waiting for passengers to discover noncompliance during a flight.¹⁸⁹ Banking supervision rests on the same logic: The Office of the Comptroller of the Currency treats examinations as fundamental, with full-scope on-site reviews on a regular supervisory cycle (generally every twelve to eighteen months).¹⁹⁰ These systems treat inspection and audit capacity as part of the legal infrastructure itself, instead of an optional, after-the-fact response to public outcry.

One might object that consumer technology is not as dangerous as nuclear reactors or commercial aviation. But the relevant axis of comparison is opacity. What nuclear plants, airlines, and consumer technology platforms share is that the regulated entity has an informational advantage that makes violations invisible to outsiders absent proactive monitoring. The question is not whether a data breach is as catastrophic as a reactor meltdown, but whether a system that relies on consumers to detect hidden harms is any more rational than one that would, for example, rely on passengers to detect mechanical failures or deficient maintenance in airplanes mid-flight.

The common thread across these regimes is institutional humility about victim awareness: the assumption that violations may be technically complex, that regulated entities will have informational advantages, and that harm may be widely distributed before any individual perceives it. Consumer protection for digital products is the conspicuous outlier. We regulate increasingly complex, sensor-rich consumer products with a system that mostly lacks routine inspection capacity for those products' hidden behaviors. There is no consumer analog of resident inspectors, mandatory black-box logging, or continuous compliance telemetry for the practices most likely to be incognito. The result is a predictable enforcement

188. *Types of FDA Inspections*, FDA (Sept. 13, 2024), <https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-basics/types-fda-inspections> [https://perma.cc/Z3MX-BRP5].

189. *Air Carrier Oversight*, FED. AVIATION ADMIN. (Mar. 31, 2022), <https://www.faa.gov/about/initiatives/sas/oversight> [https://perma.cc/CC4G-HEWR] (describing the Federal Aviation Administration's certification and surveillance responsibilities for air carriers).

190. OFF. OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: BANK SUPERVISION PROCESS 12 n.18 (2019), <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/bank-supervision-process/pub-ch-bank-supervision-process.pdf> [https://perma.cc/2MC2-M34Y] ("12 USC 1820(d) requires the OCC to conduct a full-scope, on-site examination of each insured depository institution every 12 or 18 months."). The FDIC and the Federal Reserve, which share responsibility for supervising banks with the OCC, follow the same schedule. *See* 12 C.F.R. § 337.12(a), (b) (FDIC); *id.* § 208.64(a), (b) (Federal Reserve).

deficiency: an entire class of profitable misconduct that rational firms can expect to commit with near-zero probability of detection.

Closing that gap requires treating detection capacity as a central design choice instead of a happy accident. In practice, that means rebuilding consumer protection around mechanisms that can generate reliable information about compliance even when no victim knows to complain, without omnipresent surveillance of every app and device. Recent scholarship on “regulatory monitoring” makes a similar point: Modern markets increasingly require institutions that can observe business practices at scale rather than treating visibility as a natural feature of harm.¹⁹¹ Sections B and C translate this principle into specific proposals for regulation and litigation respectively. In short, when the legal system makes concealment cheap, rational firms will conceal. When it makes concealment risky and costly, incognito consumer harm becomes harder to sustain and much less profitable.

B. Regulatory Reforms: Public Detection and Deterrence

Section A argued that consumer protection must shift from fire alarm to police patrol oversight; Section B proposes three mechanisms to operationalize that shift. Because incognito consumer harm suppresses complaints, regulators cannot treat consumer reports as the default trigger. Public enforcement needs tools that generate credible compliance information even when no one complains and that make concealment an aggravating factor instead of a liability shield. Three reforms—targeted transparency rights that function as low-level audits, auditability by design through logging and telemetry, and stronger audit and whistleblower infrastructure—would begin this transition without requiring permanent, omnipresent surveillance.

1. Data Transparency Rights with Teeth

Modern privacy law already gives consumers rights to know what data firms hold and to request deletion. The California Consumer Privacy Act¹⁹²

191. See, e.g., Van Loo, *supra* note 16, at 1631 (discussing how firms like Google and Meta are “unusually shielded from observation”); David L. Markell & Robert L. Glicksman, *A Holistic Look at Agency Enforcement*, 93 N.C. L. REV. 1, 55–56 (2014) (“Among the factors that have made effective enforcement more daunting for some agencies and programs are an increase in the number of regulated entities; increases in regulatory responsibilities and mandates for agencies and regulated entities alike; implementation of programs that depend on making difficult causal connections between regulated activities and environmental harms . . .”).

192. CAL. CIV. CODE §§ 1798.105, 1798.110, 1798.115, 1798.130 (West 2026).

and the European Union's General Data Protection Regulation¹⁹³ are the most prominent examples. However, while these rights matter for reasons of dignity and autonomy, they are weak as standalone detection tools. Consumers rarely know when to exercise them, firms operationalize the "weakest versions,"¹⁹⁴ and incognito consumer harm exacerbates both problems: If wrongdoing is concealed, most consumers will not know when to ask, and firms can treat the rights process as another site for obfuscation.¹⁹⁵ In one investigation, Honey's malicious data collection was revealed because the company left its source code exposed and an anonymous person sent it to a journalist.¹⁹⁶

While transparency rights remain valuable, they must be redesigned to produce legally consequential signals about hidden conduct. The central design choice would be to convert a consumer's inquiry into a legally consequential audit prompt. Legislatures can create a narrow "verification right," which would be the right to demand a sworn, auditable answer to specific binary questions: for example, whether the firm still possesses identity-verification documents it promised to delete, whether it shared or granted access to sensitive data, or whether any automated system used protected traits in decisions about the user. The point is to design questions that test checkable propositions for which a false answer is itself evidence of concealment. In practice, the response could be required to be signed or digitally attested by a compliance officer and supported by a minimal basis statement referencing record-keeping categories such as deletion logs or access logs. If a firm refuses to respond or gives a materially false response,¹⁹⁷ liability would attach even if the consumer could not prove downstream misuse of their own data. The injury is the denial of verifiable truth in a context where concealment is the mechanism of harm.

The verification right needs an enforcement lever that does not depend on proving downstream harm, the very problem hobbling victims in the status quo. Liquidated damages calibrated to concealment fit this need.

193. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 15, 2016 O.J. (L 119) 1, 43.

194. Margot E. Kaminski, Essay, *The Case for Data Privacy Rights (or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 386 (2022).

195. Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 1002 (2023) ("Access rights, however, fall short . . . [I]ndividuals will face too great a burden to access and review all important records. The onus should not be on individuals to continually act as unpaid proofreaders of their records.").

196. MEGALAG, *supra* note 1, at 00:25 (relating that an "anonymous source found the code and sent it" to MegaLag).

197. As for how consumers or regulators would know whether a company lied, this Article proposes telemetry, audits, and whistleblower incentives. *See infra* Sections III.B.2–3.

Illinois's Biometric Information Privacy Act provides a useful template: It authorizes liquidated damages of \$1,000 for negligent violations and \$5,000 for intentional or reckless violations, plus attorneys' fees.¹⁹⁸ A consumer protection analog could impose statutory damages for false or materially incomplete verification responses, with higher penalties for willful concealment. The damages need not try to measure the value of privacy harm. The point is to deter concealment by creating predictable per-person consequences for lying about regulated practices.

The verification right's viability in federal court depends on how it interacts with *TransUnion*'s concreteness requirement. A firm might argue that a consumer who receives a false verification response but cannot show downstream misuse lacks a "concrete" injury sufficient for Article III standing. Such a concern largely dissolves in state court, where Article III does not apply and legislatures can define actionable injury subject to state standing requirements.¹⁹⁹ Illinois's Biometric Information Privacy Act, the model for the liquidated damages structure proposed here, has been enforced in state courts beyond *TransUnion*'s reach.²⁰⁰ Even at the federal level, the objection can be addressed. As argued in Section II.B, *TransUnion*'s framework is itself part of the structural problem this Article identifies; it rewards concealment when plaintiffs cannot establish the concrete injury it demands. But even on the decision's own terms, a false verification response differs from the mailing-format violations at issue in *TransUnion*: The defect concerns the truth of the answer, not merely its format.²⁰¹ It is a directed misrepresentation delivered to a specific consumer who requested a truthful answer—conduct that is particularized by nature and may support an analogy to common-law fraud and deceit when reliance on the false answer causes concrete harm.²⁰² The broader tension between statutory damages and Article III standing recurs for the litigation reforms proposed in Section III.C below.

The verification right should also be narrow by design. Its purpose is not generalized discovery but targeted compliance testing in domains where concealment is the primary enforcement obstacle. Accordingly, it can be

198. 740 ILL. COMP. STAT. ANN. 14/20 (West 2026).

199. *ASARCO Inc. v. Kadish*, 490 U.S. 605, 617 (1989) ("[T]he state courts are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law.").

200. See *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1207 (Ill. 2019) (holding that a BIPA plaintiff may seek liquidated damages without alleging injury beyond the violation of statutory rights).

201. See *TransUnion LLC v. Ramirez*, 594 U.S. 413, 438–42 (2021).

202. See *id.* at 425, 432 (identifying "harms traditionally recognized as providing a basis for lawsuits in American courts," including "the tort of defamation" as an example of a harm with a "close relationship" to concrete Article III injury).

limited to specified high-risk categories (such as biometrics, precise location, intimate images, children's data, and identity verification documents), to firms above a size threshold, or to practices that are already regulated but hard to detect—data retention promises, access restrictions, and profiling constraints. Familiar limiting principles from existing access rights regimes, such as protections for trade secrets and third-party rights,²⁰³ can provide additional safeguards. The purpose is to create a low-cost, high-leverage mechanism for puncturing secrecy in the subset of settings where secrecy is itself the compliance strategy, without forcing the public disclosure of proprietary code or turning every consumer into a litigant.

Finally, verification rights work best when paired with a public backstop. Rather than requiring every individual request to trigger a sworn corporate response—an obligation that would be burdensome and politically implausible at scale—the mechanism should operate as a tiered petition. At the first tier, consumers could ask specific binary questions in regulated high-risk domains: whether the firm retained documents it promised to delete, shared or granted access to sensitive data, or used protected traits in an automated decision about the user. The firm's ordinary response would be standardized and tied to recordkeeping categories such as deletion, access, or decision logs. At the second tier, clustered requests concerning the same firm or practice would trigger escalation: a sworn response to the questions raised and, where warranted, regulator authority to initiate a compulsory audit. The design builds on familiar public enforcement tools, including subpoenas, civil investigative demands, and compulsory requests for documents, testimony, or written answers.²⁰⁴ The verification right proposed here would extend a similar logic to the consumer context, creating a structured pipeline from private skepticism to public investigation.

2. *Telemetry and Mandatory Monitoring for Risky Systems*

Some incognito harms are not discoverable through consumer inquiries alone. If a device covertly records audio, or a service silently scrapes camera roll photos,²⁰⁵ consumers may not even know what to ask until after a leak

203. See, e.g., Regulation 2016/679, *supra* note 193, recital 63, 2016 O.J. (L 119) at 12 (trade secrets protection).

204. See, e.g., N.Y. EXEC. LAW § 63(12) (McKinney 2026) (authorizing the attorney general to take proof and issue subpoenas); 15 U.S.C. § 57b-1(c)(1), (c)(11) (authorizing FTC civil investigative demands for documents, tangible things, written reports or answers, and oral testimony, and requiring sworn certifications or answers under oath).

205. See *The Accidental Hacker: How One Man Gained Control of 7,000 Robots*, *supra* note 4; Oestreicher, *supra* note 7.

or breach reveals the practice. In this case, the regulatory problem goes beyond information asymmetry because the underlying systems lack auditability. The solution is to require verifiable compliance exhaust: logs, telemetry, and record-keeping that make it possible for someone other than the firm to check what happened.

The idea is familiar from safety regulation. Black boxes exist because we cannot rely on the regulated entity's voluntary recollection after the fact. In aviation, flight data and cockpit recorders have long been required to ensure objective post-incident information.²⁰⁶ Consumer technology needs an analog for certain high-risk practices. The EU has begun operationalizing this logic in digital regulation. The EU Artificial Intelligence Act requires high-risk AI systems to support automatic logging over the system's lifetime and gives competent authorities access upon reasoned request.²⁰⁷ The EU Digital Services Act requires annual independent audits for large online platforms.²⁰⁸ The common principle is that, beyond prohibiting conduct, the law must require the preconditions for verifying compliance. A U.S. analog need not copy these regimes wholesale. The EU Digital Markets Act, which provides for proactive monitoring through defined investigative timeframes,²⁰⁹ has been criticized for requiring regulators to obtain information that cannot realistically be obtained or kept current.²¹⁰ But, unlike the execution, the motivating concern is valid: Where harm is easy to hide, compliance must be made inspectable.

In the United States, agencies already have partial building blocks for proactive information gathering. The FTC can compel information through its Section 6(b) authority, which authorizes it to require entities to file "annual or special" reports or answers to specific questions about their "organization, business, conduct, [and] practices."²¹¹ In 2024, the FTC

206. See 14 C.F.R. § 121.343 (2025).

207. Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), arts. 12, 21(2), 2024 O.J. (L 144) 1.

208. Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), art. 37, 2022 O.J. (L 277) 1.

209. Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), art. 17, 2022 O.J. (L 265) 1; European Commission Press Release IP/25/2675, Commission Opens Investigation into Potential Digital Markets Act Breach by Google in Demoting Media Publishers' Content in Search Results (Nov. 12, 2025) (saying the Commission aims to conclude the investigation in twelve months).

210. See Yunsieg P. Kim, *A Revolution Without a Cause: The Digital Markets Act and Neo-Brandeisian Antitrust*, 2023 WIS. L. REV. 1247, 1255–56.

211. 15 U.S.C. § 46(b).

voted to use 6(b) compulsory process to study “surveillance pricing,” focusing on intermediaries that market data- and AI-driven tools for individualized pricing.²¹² The FTC has also published early staff perspectives on that 6(b) study.²¹³ Whatever one may think of the FTC’s ultimate policy choices—and opinions are clearly divided²¹⁴—the institutional point is that 6(b) can be used to map opaque markets *ex ante* rather than waiting for the first whistleblower or lawsuit. But 6(b) is not a substitute for auditability by design. A regulator can ask questions, but it cannot reliably verify answers if the underlying systems keep no records.

For discrete high-risk categories of harm, Congress and states should require audit trails as a condition of operation. If firms can profit by building systems that cannot be audited, they likely will. If the law makes auditability part of the compliance obligation, much like record-keeping duties in other regulatory domains, it can change the engineering incentive: Secrecy becomes costlier than simply obeying the law. Regulators could require and periodically audit tamper-resistant logs of (1) access to sensitive repositories (who accessed what and when); (2) retention and deletion events for data that firms routinely promise to delete (verification IDs, voiceprints, and intimate images); and (3) automated decision events for regulated uses (when an algorithm uses or infers protected traits in pricing or eligibility decisions). These logs need not be public. They can be confidential, available only to regulators or certified independent auditors under strict security requirements. The goal is to ensure that, when a practice is illegal, the perpetrator cannot also make it unknowable.

Two safeguards are crucial. First, telemetry must be risk based and data minimizing. Logs can often be stored as hashes, counters, or event metadata that shows whether a forbidden action occurred without recording the

212. *6(b) Orders to File Special Report Regarding Surveillance Pricing Involving Intermediary Companies*, FTC (July 19, 2024), <https://www.ftc.gov/reports/6b-orders-file-special-report-regarding-surveillance-pricing-involving-intermediary-companies> [<https://perma.cc/B2XQ-DMH2>].

213. FTC, *ISSUE SPOTLIGHT: THE RISE OF SURVEILLANCE PRICING* (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/sp6b-issue-spotlight.pdf [<https://perma.cc/9RNT-TUNF>].

214. See, e.g., Zephyr Teachout, *The Long Future of the Neo-Brandeisian Movement*, in *Three Parts*, 2024 NETWORK L. REV. 124, 127 (praising the FTC under Chair Lina Khan as “pragmatic, grounded, and reality-based” and arguing that its policy direction has signaled “a transformative shift in how we understand and enforce antitrust law”); Daniel A. Crane, Essay, *Neo-Brandeis Goes to Washington: A Provisional Assessment of the Biden Administration’s Antitrust Record*, 111 VA. L. REV. ONLINE 215, 216 (2025) (“[N]eo-Brandeisians did attempt dramatic reform in many ways[,] . . . advancing novel or ‘edgy’ theories in merger and non-merger cases, and, especially, testing the FTC’s rulemaking authority through an aggressive rule prohibiting employment non-compete agreements. But the neo-Brandeisians leave Washington with relatively little to show for these efforts.”).

underlying content.²¹⁵ Second, access must be controlled and confidential. Genuine concerns regarding trade secrets and privacy can be addressed through mechanisms routinely used elsewhere: limited-purpose access, secure data rooms, protective orders, and sanctions for unauthorized disclosure.²¹⁶ The goal is to ensure that companies cannot evade accountability by designing systems with no built-in audit trail, without giving regulators access to private communications.

3. *Proactive Audits and Whistleblower Incentives*

Even with verification rights and telemetry, regulators will miss what they are not looking for. Incognito consumer harm thrives on novelty: new intermediaries, new data uses, and new forms of obfuscation. A detection-first system thus needs multiple “sensors” beyond consumer complaints, like proactive audits, insiders, competitors, and researchers. Without sensors, the police patrol system risks regressing into the unreliable and inefficient system that Robert Bork called the “good old American tradition of the sheriff of a frontier town: he did not sift evidence, distinguish between suspects, and solve crimes, but merely walked the main street and every so often pistol-whipped a few people.”²¹⁷

Start with audits. In many consumer domains, U.S. regulators lack the kind of routine examination authority that makes police patrol oversight operational.²¹⁸ But they can approximate it through a mix of (1) risk-based technical audits, (2) compulsory reporting targeted at high-risk practices, and (3) sustained investment in in-house technologists who can interpret what they find. The goal is to audit where incentives to conceal are high and external visibility is low, such as online devices with microphones and cameras, ID-verification pipelines, and pricing systems built on consumer

215. See, e.g., Ahmed I. Taloba & Alanazi Rayan, *A Privacy Preserving Medical Data Management Framework Using Blockchain Enabled Encrypted Role Based Access Control*, 15 SCI. REPS., art. no. 43864 (2025) (describing auditable logs and encrypted role-based access controls that limit disclosure of sensitive metadata).

216. See, e.g., *FTC v. Sysco Corp.*, 83 F. Supp. 3d 1, 5 (D.D.C. 2015) (secure data rooms); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1353 (2018) (proposing “protective orders to limit the use and distribution of trade secrets beyond the needs of the proceeding”).

217. ROBERT H. BORK, *THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF* 6 (1978).

218. Cf. Willis, *supra* note 47, at 1397–98 (arguing the proposed reform “for performance-based consumer law would produce fairer outcomes than . . . [the] complaint-driven enforcement” that characterizes the status quo); see also *supra* Section II.A.3 (discussing reliance of federal and state consumer protection law enforcement on consumer complaints and other alarm bells).

surveillance, rather than to inspect every app on the market.²¹⁹ Algorithmic impact-assessment literature makes the related point that audits and assessments are governance tools only to the extent that systems exist to enforce them and learn from them over time.²²⁰

Next, incentivize third-party detection. Hidden corporate misconduct can be exposed by competing firms or independent researchers long before regulators ever suspect anything amiss.²²¹ The relevant “whistleblower” need not always be an individual employee. In many digital markets, app stores, cloud providers, payment processors, analytics vendors, auditors, and other value-chain actors may be better positioned than consumers to see whether a firm’s public promises match its technical behavior. These actors also have reputational and contractual incentives that individual consumers lack: A platform that markets itself as privacy protective, for example, may benefit from exposing or excluding downstream partners whose practices threaten that brand position. A detection-first regime should therefore treat value-chain intermediaries as potential information-forcing gatekeepers, using safe harbors, reporting channels, and contractual compliance obligations to encourage disclosure.

Dark patterns research also shows what third-party expertise can reveal. In some cases, the consumer cannot say more than “this was confusing” or “I gave up,” but an expert can map the user journey, identify repeated friction points, compare design alternatives, and show that the interface was structured to suppress exit, consent, or objection. That evidence may not by itself establish liability, but it is highly relevant to detection. It helps convert a consumer’s inchoate frustration into a design-level account of how invisibility was produced.

219. See, e.g., Gillis, *supra* note 120, at 133 (“Firms tend to conceal their pricing policies, particularly when they engage in practices like PD that could cause consumer backlash.”); Michele Estrin Gilman, Essay, *Me, Myself, and My Digital Double: Extending Sara Greene’s Stealing (Identity) from the Poor to the Challenges of Identity Verification*, 106 MINN. L. REV. HEADNOTES 301, 321 (2022) (“[T]he states’ outsourcing of identity verification to third-party vendors lacked transparency and blurred lines of accountability.”); Graham Johnson, Note, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345, 353 (2019) (“Manufacturers of IoT products have little interest in disclosing . . . just how much data manufacturers are collecting about consumers . . .”).

220. See, e.g., Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117, 118 (2021) (describing the objectives of impact assessment as early mitigation of social effects and documentation for future learning).

221. See, e.g., Myron Levin, *Rival’s Tip Led EPA to Penalize Pesticide Firm in Chatsworth*, L.A. TIMES (June 13, 1985), <https://www.latimes.com/archives/la-xpm-1985-06-13-me-10713-story.html> [<https://perma.cc/6BV8-7LB2>] (discussing how an EPA penalty for illegal marketing “resulted from a tip from a rival distributor”); MEGALAG, *supra* note 1 (discussing how an independent journalist exposed Honey).

But the legal environment can make this work perilous. A modest but meaningful step is to expand safe harbors for good-faith security research. The Department of Justice recently adopted a charging policy for the Computer Fraud and Abuse Act that directs prosecutors not to charge “good-faith security research,” defined as access solely for testing, investigation, and correction of security flaws, carried out in a way designed to avoid harm and used primarily to promote security or safety.²²² Clarifying the liability landscape for responsible research would improve the odds that hidden abuses are uncovered by someone other than a hacker with malicious intent.

Finally, and most critically, a detection-first regime must protect and reward insiders. Incognito consumer harm is frequently revealed not by victims but by people with access, such as engineers, compliance staff, contractors, and auditors. Recent scholarship on tech whistleblowing emphasizes that “[r]adical information asymmetries” make internal disclosures a de facto source of governance information “in the absence of meaningful, rigorous, and systematic transparency rules.”²²³ In an incognito world, whistleblowing is an indispensable infrastructure. The dearth of whistleblower provisions in consumer protection law²²⁴ and, where such provisions exist, the dearth of monetary rewards for whistleblowers²²⁵ are particularly quaint, given that whistleblower programs with money rewards are used in many other domains. The SEC’s whistleblower program authorizes awards of 10 to 30 percent of monetary sanctions collected in successful enforcement actions.²²⁶ The False Claims Act uses qui tam relators to expose fraud that the government would otherwise miss, rewarding successful relators with a share of recoveries.²²⁷ These regimes recognize a premise that translates well to incognito consumer harm: When violations are hard to observe from outside, internal informants are often the cheapest, most effective, or even only detectors.

222. Press Release, U.S. Dep’t of Just., Department of Justice Announces New Policy for Charging Cases Under the Computer Fraud and Abuse Act (May 19, 2022), <https://www.justice.gov/archives/opa/pr/departments-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act> [<https://perma.cc/2AMR-EN45>].

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

224. There are no whistleblower or anti-retaliation provisions in the FTC Act, 15 U.S.C. §§ 41–58; the Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x; or the Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692–1692p.

225. The Consumer Product Safety Improvement Act and the Consumer Financial Protection Act prohibit reprisals, but do not give money rewards. See 15 U.S.C. § 2087; 12 U.S.C. § 5567.

226. 15 U.S.C. § 78u-6(b)(1).

227. 31 U.S.C. § 3730(d).

A detection-first consumer protection regime should therefore strengthen anti-retaliation protections, create confidential reporting channels to agencies with technical staff who can evaluate tips, and offer money rewards scaled to social value—especially for evidence of deliberate concealment, repeat violations, or practices affecting sensitive populations such as children, patients, and targets of discriminatory profiling. Rewards can be financed from penalties recovered in successful actions, as in other regimes. To avoid perverse incentives, eligibility can be conditioned on responsible disclosure, preservation of evidence, and cooperation with investigators.

These three regulatory mechanisms—verification rights, auditability by design, and whistleblower infrastructure—address the supply side of detection: generating information about compliance that the current system lacks. In short, when the legal system makes concealment cheap, rational firms will conceal. When the law makes concealment risky and costly, incognito consumer harm becomes harder to sustain. Section C turns to the demand side: ensuring that private litigation can translate detection into accountability when public enforcement falls short.

C. Litigation Reforms: Unmasking Harm in Private Enforcement

Section B addressed the supply side of detection: generating compliance information that the current system lacks. But even the best-resourced regulators will miss violations, for reasons no more sinister than the inevitable imperfection of deterrence.²²⁸ Private litigation supplies a second channel of enforcement via deterrence, compensation, and public airing of facts that perpetrators would prefer to keep buried. Yet incognito consumer harm is engineered to defeat the basic premises of civil litigation—that plaintiffs can discover enough facts to plead, establish a cognizable injury, and aggregate low-value claims into a viable enforcement vehicle. The reforms below aim to make concealment backfire, while giving plaintiffs a path to the minimum information needed to litigate without turning every case into open-ended discovery.

1. Penalize Concealment-by-Design as Constructive Spoliation

Part II showed that spoliation doctrine is inoperative for incognito harm because preservation duties attach only once litigation is foreseeable, while

228. Alex Raskolnikov, *Irredeemably Inefficient Acts: A Threat to Markets, Firms, and the Fisc*, 102 GEO. L.J. 1133, 1157 (2014) (noting even “the optimal regulation” must assume that “irredeemable acts . . . cannot be perfectly deterred”).

incognito harm often prevents litigation from becoming foreseeable. A targeted solution is to treat intentional concealment that impairs proof as a spoliation analog, which I call constructive spoliation, and attach litigation consequences once concealment is shown. When a defendant's design, notice, or recordkeeping choices are plausibly aimed at keeping a violation undiscoverable, courts should treat invisibility as an aggravating wrong rather than a neutral fact.

Operationally, courts could implement constructive spoliation through predictable, cabined tools. The first potential tool is evidentiary presumptions tied to concealment. Plaintiffs who make a threshold showing—through internal documents, whistleblower testimony, technical analysis, or admissions in parallel proceedings—that a firm designed its product, notice architecture, or recordkeeping system to prevent detection could obtain adverse inferences and presumptions ordinarily tied to preservation duties. The presumption need not decide the case, and it can be limited to the proposition most directly undermined by concealment. For example, if a company's system auto-deletes access logs that would reveal unauthorized employee viewing of sensitive video,²²⁹ a court could presume that unauthorized access did occur in the relevant period, subject to rebuttal. Likewise, if a firm intentionally designs required "notice" to land in spamboxes,²³⁰ courts could presume non-notice for purposes of tolling, assent, and waiver.

This is hardly a drastic reform. Existing rules already authorize adverse presumptions and similar sanctions upon a finding of "intent to deprive,"²³¹ and longstanding doctrine presumes that any destroyed evidence was adverse to the perpetrator.²³² The main obstacle to applying spoliation logic to concealment-by-design under existing law is the idea that product design changes occurred before litigation was foreseeable. But this temporal distinction confuses sequence with substance. Destroying evidence once litigation is pending and engineering concealment to prevent litigation both ensure that evidence of wrongdoing is destroyed. Therefore, when intent to conceal wrongdoing by product design is compelling, courts should treat it as constructive spoliation.

The second tool is burden shifting on the facts that concealment makes unknowable. Incognito harm turns litigation into a contest over information

229. See Complaint, *supra* note 151, at 6–7.

230. See Kim, *supra* note 69, at 613–35.

231. See FED. R. CIV. P. 37(e)(2); *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590–95 (4th Cir. 2001) (affirming dismissal of lawsuit as sanctions after spoliation prejudiced adversary).

232. See, e.g., *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 437 (S.D.N.Y. 2004) (describing adverse inference instruction given to jury regarding evidence destroyed by defendant).

asymmetries. Was personal information accessed? Was it shared? Was it retained past deletion promises? Did an algorithm use prohibited traits? When a defendant's own concealment makes those questions unanswerable for outsiders, the ordinary allocation of burdens can reward obstruction. A constructive spoliation approach would shift burdens on precisely the elements for which proof is missing because of the defendant's concealment. This is a familiar response when a party's own wrongful conduct prevents ordinary proof.²³³ The trigger must be a meaningful threshold showing of intentional concealment, not mere complexity or ordinary confidentiality.

Recent consumer protection law literature has proposed responding to modern information asymmetry with burden shifting, but it still presupposes that a plaintiff (or regulator) can first uncover enough outward evidence to trigger the shift—a premise that breaks down for incognito harm. For example, Professors Susan Block-Lieb and Edward Janger would treat a showing of disparate impact or predatory outcomes as an “impact” trigger that forces the lender to come forward with evidence that its AI-driven practices are fair and nondiscriminatory.²³⁴ That suggestion would be helpful where the harm is legible in observable patterns or contract terms. But incognito consumer harm is engineered precisely to prevent those patterns from becoming visible in the first place. If the contested fact is whether data were accessed, retained, or repurposed in a way that outsiders cannot detect, there may be no measurable impact to plead or prove at the threshold, so the burden would not shift. This only reinforces the need for a constructive spoliation approach. When a defendant's concealment architecture is the reason that key elements are hidden, concealment itself must supply the trigger to reallocate burdens, rather than waiting for outward manifestations that incognito harm strategies are designed to suppress.

A third tool to penalize concealment as constructive spoliation is to implement concealment-sensitive tolling and waiver rules. Incognito harm often works simply by running out the clock, in that a practice is designed to remain hidden until limitations periods, opt-out windows, or cancellation rights have lapsed. Courts already recognize doctrines like fraudulent

233. See, e.g., *Anderson v. Mt. Clemens Pottery Co.*, 328 U.S. 680, 687–88 (1946) (shifting burdens where defendant's failure to keep records made precise proof impossible), *superseded by statute in part*, Portal-to-Portal Act of 1947, Pub. L. No. 80-49, 61 Stat. 84 (codified as amended at 29 U.S.C. §§ 251–262).

234. Susan Block-Lieb & Edward J. Janger, *Impact Ipsa Loquitur: A Reverse Hand Rule for Consumer Finance*, 45 *CARDOZO L. REV.* 1133, 1135–36 (2024) (arguing evidence of disparate impact/predatory outcomes should trigger burden shifting to defendants to justify fairness).

concealment and equitable tolling in certain settings,²³⁵ but the dominant pattern of incognito consumer harm warrants a clearer, more pro-plaintiff default rule. Where a defendant's conduct plausibly impeded detection, tolling should be presumed unless the defendant shows that a reasonable consumer actually had practical notice and opportunity to act. Otherwise, firms can exploit the same information asymmetry twice: first to keep harm hidden, and then to argue that it was discovered "too late." The 23andMe arbitration clause discussed in Part II illustrates the tactic: A company mass-emails a mandatory arbitration clause with a thirty-day opt-out window, likely designed to land in spamboxes, and then invokes the waiver against consumers who never saw the email.²³⁶

These solutions are deliberately modest. They do not require creating a free-floating new tort everywhere. They simply ensure that, once concealment is credibly alleged and supported, courts do not let the defendant exploit the informational asymmetry that it created itself. There still may be overbreadth concerns: Firms might argue that any effort to minimize legal exposure such as limited logging, guarded disclosures, or confidentiality could be reframed as "concealment." The answer is to limit constructive spoliation to affirmative concealment signals, such as internal directives to avoid detection, engineering choices that delete compliance-relevant audit trails while preserving business-relevant data, obfuscatory notification language, or intentional routing of notices through channels likely to be missed—not mere complexity or imperfect compliance. While making this distinction may well be a painstaking thing to do in practice, there is plenty of precedent—up to the U.S. Supreme Court—where civil liability and penalties turn on the degree of unlawful intent reflected in how a technology is designed or used.²³⁷

2. *Allow Limited Pre-Suit and Motion-Stage Discovery for Incognito Claims*

Part II showed that plausibility pleading²³⁸ creates a catch-22 for incognito harm because the most probative facts are often held exclusively by the defendant, but plaintiffs cannot plead what they cannot observe. If

235. See, e.g., *Holmberg v. Armbrrecht*, 327 U.S. 392, 396–97 (1946) (recognizing equitable tolling in federal law where fraud concealed the cause of action).

236. See Dixit, *supra* note 109; Kim, *supra* note 69, at 613–35.

237. See, e.g., *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919 (2005) (“[O]ne who distributes a device with the object of promoting its use to infringe copyright . . . is liable for . . . infringement by third parties.”).

238. See *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556–58 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678–80 (2009).

the legal system wants private enforcement to function for hidden harms, it needs a narrow mechanism for plaintiffs to obtain the minimum facts necessary to plead without authorizing fishing expeditions.

A workable model is cabined pre-suit or early-stage discovery: targeted information-forcing on specific, checkable questions. U.S. law has building blocks for such a model, but they are underpowered for incognito harm. Federal Rule of Civil Procedure 27 allows pre-suit depositions to perpetuate testimony, not to investigate whether wrongdoing occurred.²³⁹ Texas's Rule 202 goes further by permitting pre-suit depositions to investigate potential claims, subject to limitations and balancing.²⁴⁰ Recent scholarship likewise supports limited pre-suit discovery to reduce information asymmetry and loss of electronically stored information that obstructs otherwise colorable claims.²⁴¹

In the incognito harm context, a calibrated procedure could operate in two steps. First, the plaintiff must present a specific, credible basis for suspicion, such as a whistleblower declaration, a published technical analysis, an agency inquiry, or an expert affidavit explaining observable signals consistent with the alleged hidden practice. The showing should be stronger than a hunch but could be weaker than the full proof that current pleading doctrine effectively demands.²⁴² Second, discovery should be narrow and question driven, limited to specific, checkable questions. For example, "Do you retain X category of data past Y date? What logs exist showing deletion? Who had access to repository Z? Did the system call a feature flag associated with the prohibited practice?" This approach avoids the open-ended "tell us everything about your algorithm" fishing expedition approach and instead would target the specific unknowns that currently make pleading impossible.

These procedures should be complemented with a carrot and a stick for defendants. The carrot would be strong protective conditions. Because defendants are likely to invoke trade secrets and security concerns, orders should default to confidentiality protections: attorney-eyes-only review, secure data rooms, neutral experts, and limits on use outside litigation.²⁴³

239. FED. R. CIV. P. 27.

240. See TEX. R. CIV. P. 202.1 ("A person may petition the court for an order authorizing the taking of a deposition . . . either . . . for use in an anticipated suit; or . . . to investigate a potential claim or suit."); *In re Jorden*, 249 S.W.3d 416, 422 (Tex. 2008) (discussing accrual and unknown essential facts in the Rule 202 context); *In re Doe*, 444 S.W.3d 603, 610–11 (Tex. 2014) (discussing Rule 202's scope and limits).

241. See, e.g., Jeffrey A. Parness, *The Roberts Court and Lost ESI*, 51 STETSON L. REV. 335, 362–64 (2022).

242. See Miller, *supra* note 158.

243. See FED. R. CIV. P. 26(c)(1) (protective orders); FED. R. CIV. P. 26(b)(1) (proportionality).

Where appropriate, courts can also require plaintiffs to bear or share costs for extraordinary technical work, which would deter abuse while still allowing meritorious claims to proceed. The stick would be a self-enforcing mechanism. If a defendant refuses to comply with early discovery or gives evasive answers, the remedy should be procedural: adverse inferences, cost shifting, or orders deeming certain facts to be established for pleading and certification purposes.

The premise of pre-suit or early-stage discovery is not that discovery should become routine before a complaint survives a motion to dismiss. The premise is that incognito harm represents a discrete class of cases where insisting on ordinary pleading proof is tantamount to immunity. A narrowly tailored “peek behind the curtain” procedure would preserve the basic screening function of pleading while preventing concealment from becoming dispositive. A further complementary tweak is to relax courts’ hostility to plaintiffs’ use of third-party investigative materials—such as agency complaints, technical reports, whistleblower filings, and prior litigation documents—to supply plausibility when defendants hold the facts. Recent scholarship on “stolen plausibility” persuasively argues that courts often unfairly penalize plaintiffs for relying on precisely the materials that can substitute for inaccessible internal facts.²⁴⁴ In the incognito context, those materials are often the only realistically available answer to a fatal information asymmetry.

3. Legislatively Make “Invisible” Injuries Actionable

Some litigation failures cannot be fixed by procedure alone because the bottleneck is substantive justiciability. Standing doctrine’s insistence on a “concrete” injury and its preference for common-law analogs can convert hidden invasions into “no injury” when courts require a further showing of harm, such as third-party disclosure or downstream misuse.²⁴⁵ The predictable result is that concealment becomes a liability shield: The better a firm is at keeping misuse internal and unobservable, the harder it would be for plaintiffs to establish standing and to certify classes. The most direct solution is legislative. If incognito harm is systematically filtered out by courts’ injury taxonomy, legislatures can make the injury explicit. There are several potential fixes, each with different costs.

The first potential solution is statutory damages for defined hidden-practice violations. Statutory damages, legislative declarations of injury,

244. See, e.g., Marcus Alexander Gadson, *Stolen Plausibility*, 110 GEO. L.J. 291, 324 (2021) (discussing courts “sanctioning plaintiffs for borrowing plausibility”).

245. See *supra* Section II.B.

and presumptions of harm would not automatically establish federal standing under *TransUnion*. Statutory damages would nevertheless do two important things. First, they would make harms redressable without individualized proof of monetary loss. Second, they would create predictable exposure that changes firm incentives *ex ante*. Illinois's Biometric Information Privacy Act is a familiar example of liquidated damages for privacy violations that are hard to value.²⁴⁶ A federal or state analog could target representative frequent examples of incognito harm, particularly in the realm of privacy: undisclosed data retention despite deletion promises, undisclosed access to sensitive repositories, or use of protected traits in regulated decisions.

The second possible fix is presumptions of harm for concealment-sensitive practices. Legislatures can also presume harm in narrow contexts, which is especially useful when the harm is the denial of truthful information needed to protect oneself. For example, if a firm promises deletion of identity verification documents but retains them, the law could presume injury from the loss of the promised deletion and the associated risk without requiring proof of third-party disclosure. This could be complemented with the third possible fix, a cause of action for "denial of verifiable compliance information." A central tactic of incognito harm is to prevent consumers from learning whether a violation occurred. Legislatures can treat that deprivation itself as actionable—an informational injury with teeth—by creating a right to a certified answer to specific compliance questions (as discussed above in the regulatory context)²⁴⁷ coupled with a private right of action when responses are false or materially incomplete. This strategy targets concealment directly without requiring courts to analogize the underlying harm to defamation or physical injury. It is also hardly far-fetched, given that recent bipartisan proposals—such as the AI Accountability and Personal Data Protection Act—would create a federal tort for data misuse and allow individuals to sue "any person or company" that "uses, sells, or exploits . . . personal data . . . without clear, affirmative consent."²⁴⁸

246. 740 ILL. COMP. STAT. ANN. 14/20 (West 2026).

247. See *supra* Section III.B.1.

248. Press Release, Josh Hawley, U.S. Sen. for Mo., Hawley, Blumenthal Unveil Bipartisan Bill Empowering Working Americans to Sue Big Tech, AI Companies for Stealing Creative Works (July 21, 2025), <https://www.hawley.senate.gov/hawley-blumenthal-unveil-bipartisan-bill-empowering-working-americans-to-sue-big-tech-ai-companies-for-stealing-creative-works/> [<https://perma.cc/N769-RBWL>]; S. 2367, 119th Cong. § 3(b)(1) (2025) ("Any individual whose covered data is appropriated, used, collected, processed, sold, or otherwise exploited without the express, prior consent of [a covered] individual . . . may bring a civil action in an appropriate district court of the United States or a State court of competent jurisdiction . . .").

Recent privacy law scholarship discussing the rise of “surveillance class actions” underscores the point of the foregoing reform proposals. Private litigation is increasingly the venue where these disputes play out, but procedural and standing barriers threaten to disable that channel unless privacy statutes are designed with litigation realities in mind.²⁴⁹ Incognito consumer harm strengthens that argument, because legislatures cannot create private enforcement while writing liability rules that presuppose visibility.

4. *Facilitate Aggregation and Representative Enforcement Without Rewarding Stealth*

Even when incognito consumer harms are actionable and pleadable, they are often low dollar per person and thus depend on aggregation. But class actions face two stealth-sensitive problems: (1) identifying injured members when injury is defined in outward-facing terms (disclosure, misuse, individual loss) and (2) litigating whether uninjured members defeat certification or narrow down class definitions. As previously discussed, *TransUnion* requires every damages recipient to have standing but left open when absent class members must demonstrate standing and how that interacts with Rule 23’s predominance inquiry.²⁵⁰ The Court’s later decision to dismiss *Labcorp v. Davis* as improvidently granted preserved the circuit split and practical uncertainty on that question.²⁵¹ A recent Congressional Research Service analysis also framed the post-*TransUnion* question as live and consequential for aggregate litigation.²⁵²

Incognito harm suggests several aggregation reforms that neither require courts to award damages to truly uninjured people nor enable stealth to immunize wrongdoing. Rule 23(c)(4) allows courts to certify common issues—such as whether a firm engaged in a concealed practice or designed a system to prevent consumer detection—while reserving individualized injury, causation, or damages questions for later proceedings. Scholars have

249. See, e.g., Nabil Shaikh, Comment, *Surveillance Class Actions: Reconstructing a Federal Data Privacy Private Right of Action*, 172 U. PA. L. REV. 865, 868 (2024) (“[S]everal procedural requirements, including Federal Rule of Civil Procedure 23 and Article III standing, often doom surveillance class actions. . . . [T]his Comment makes several substantive recommendations for a federal privacy law that can give effect to a private right of action.”).

250. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 n.4 (2021).

251. *Lab’y Corp. of Am. Holdings v. Davis*, 605 U.S. 327, 327 (2025); *id.* at 328 (Kavanaugh, J., dissenting).

252. BRYAN L. ADKINS, CONG. RSCH. SERV., LSB11317, SUPREME COURT CONSIDERS WHETHER FEDERAL COURTS MAY CERTIFY CLASS ACTIONS WHEN SOME PROPOSED CLASS MEMBERS ARE UNINJURED 2–3 (May 27, 2025), <https://www.congress.gov/crs-product/LSB11317> [<https://perma.cc/6Q55-ZJNM>].

advocated issue certification as a way to preserve common conduct questions without allowing individualized remedial issues to defeat certification altogether.²⁵³ To be sure, the device is not a cure-all: The certified issue must materially advance the litigation, and careless bifurcation can create inefficiency, settlement pressure, or preclusion problems.²⁵⁴ But for incognito consumer harm, where the core dispute is whether a concealed practice existed and was structured to evade detection, issue certification offers a natural fit. It can prevent defendants from leveraging “some members might be uninjured” into total defeat of certification in cases where the core conduct is uniform and the primary disputes are common.

Another possible reform is to designate representative plaintiffs beyond individual consumers. If incognito harm is defined by victim ignorance, the law should not rely only on individual victims as the gatekeepers of enforcement. Legislatures can expand *parens patriae* authority (state attorneys general suing on behalf of residents), authorize certain consumer organizations to bring representative actions, or create limited “private attorney general” models for specific hidden practices. Similar representative plaintiff models have been proposed in other areas of civil litigation²⁵⁵ and can be adapted to incognito consumer harms. These models do not eliminate the need for careful remedies, but they can reduce the dependence on individuals discovering harm and suing. State enforcement may also offer a path forward when claims proceed in state court because state courts are not always constrained by federal Article III doctrine, though state standing doctrines vary and should not be treated as uniformly permissive.²⁵⁶

New York v. TikTok illustrates why representative enforcement is especially necessary for incognito consumer harm, and why it is actively

253. See FED. R. CIV. P. 23(c)(4); Myriam Gilles & Gary Friedman, *The Issue Class Revolution*, 101 B.U. L. REV. 133, 138–39, 188–89 (2021); Myriam Gilles & Gary Friedman, *Rediscovering the Issue Class in Mass Tort MDLs*, 53 GA. L. REV. 1305, 1307–08, 1331–34 (2019).

254. See Elizabeth Chamblee Burch, *Constructing Issue Classes*, 101 VA. L. REV. 1855, 1858–60 (2015) (discussing doctrinal, logistical, preclusion, settlement, fee, and Seventh Amendment concerns).

255. See, e.g., Margaret S. Thomas, *Parens Patriae and the States’ Historic Police Power*, 69 SMU L. REV. 759, 796 (2016) (advocating for expansion of *parens patriae* in mass tort litigation by, among others, victims of cigarettes); David E. Adelman & Jori Reilly-Diakun, *Environmental Citizen Suits and the Inequities of Races to the Top*, 92 U. COLO. L. REV. 377, 441 (2021) (suggesting “lowering the barriers to filing citizen suits”); Gonzalo E. Rodriguez, Note, *The Qui Tam Environmentalist: Holding Polluters Accountable Through the False Claims Act*, 9 ALA. C.R. & C.L. L. REV. 473, 476 (2018) (exploring how to “use the *qui tam* provision . . . against those who make false representations in environmental studies”).

256. See *ASARCO Inc. v. Kadish*, 490 U.S. 605, 617 (1989) (noting that Article III constraints do not apply to state courts in the same manner).

contested. In October 2024, the New York Attorney General sued TikTok under Executive Law Section 63(12) and General Business Law Sections 349 and 350, alleging that the platform deployed addictive design features invisible to users that harm minors' mental health, such as variable reward notification schedules, autoplay, infinite scroll, and engagement-maximizing algorithmic recommendations.²⁵⁷ TikTok's own internal research found that roughly thirty-five minutes of use, as few as 260 short videos watched in rapid succession, was "the precise amount of viewing it takes for someone to form a habit"²⁵⁸—in other words, an addiction. Internal communications acknowledged that "[m]inors do not have executive function to control their screen time" and that TikTok's sixty-minute screen time tool reduced daily usage by only about 1.5 minutes, with a project manager stating that the tool's real goal was "improving public trust" through "media coverage," not reducing usage.²⁵⁹

The trial court denied TikTok's motion to dismiss on the main consumer protection counts,²⁶⁰ and TikTok has appealed to the First Department of the Appellate Division, placing the viability of the Attorney General's enforcement theory (and, implicitly, the *parens patriae* model for incognito consumer harm) squarely before an appellate court.²⁶¹ This is a textbook case for representative enforcement. The harm-causing mechanisms are embedded in algorithmic design that users, especially minors, cannot perceive—let alone trace to specific design choices. Individual users cannot sue over what they cannot see, and the fire alarm model failed. Accordingly, the state stepped in on their behalf.

257. Press Release, Letitia James, Att'y Gen. of N.Y., Attorney General James Sues TikTok for Harming Children's Mental Health (Oct. 8, 2024), <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-tiktok-harming-childrens-mental-health> [<https://perma.cc/ZKJ3-CCAS>]; Complaint, *People v. TikTok Inc.*, No. 452749/2024 (N.Y. Sup. Ct. Oct. 8, 2024).

258. Bobby Allyn, Sylvia Goodman & Dara Kerr, *Inside the TikTok Documents: Stripping Teens and Boosting 'Attractive' People*, NPR (Oct. 16, 2024, at 20:49 ET), <https://www.npr.org/2024/10/12/g-s1-28040/teens-tiktok-addiction-lawsuit-investigation-documents> [<https://perma.cc/GM2F-EVSS>].

259. Bobby Allyn, Sylvia Goodman & Dara Kerr, *TikTok Executives Know About App's Effect on Teens, Lawsuit Documents Allege*, NPR (Oct. 11, 2024, at 05:30 ET), <https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed> [<https://perma.cc/F5NK-D2VJ>].

260. Decision and Order on Motion, *People v. TikTok Inc.*, No. 452749/2024 (N.Y. Sup. Ct. May 29, 2025) (denying dismissal of Counts I–IX while striking COPPA compliance and Chinese government allegations).

261. Notice of Appeal, *People v. TikTok Inc.*, No. 452749/2024 (N.Y. App. Div. June 30, 2025); compare *Patterson v. Meta Platforms, Inc.*, 239 N.Y.S.3d 726, 734 (N.Y. App. Div. 2025) (treating algorithmic recommendations as protected publishing activity under Section 230), with *Anderson v. TikTok, Inc.*, 116 F.4th 180, 184 (3d Cir. 2024) (holding Section 230 did not bar claims based on TikTok's own algorithmic recommendations). A decision favorable to the Attorney General would validate the state enforcement model for incognito consumer harm; a decision favorable to TikTok would illustrate the urgency of the legislative reforms this Article proposes.

One might object that the TikTok case is not a genuine example of incognito consumer harm because the harm was eventually exposed. But the exposure owed little to the legal system's ordinary detection channels. A multistate investigation launched in 2022 was in significant part a product of the extraordinary geopolitical scrutiny that TikTok attracted because of its Chinese ownership, culminating in the Supreme Court unanimously upholding a divestiture law in January 2025.²⁶² That geopolitical spotlight generated the political momentum for state investigations that might not otherwise have occurred. Even then, the most damaging internal admissions became public only by accident. When the Kentucky Attorney General's office sued in October 2024, it used faulty PDF redaction—blacked-out text that could be revealed by copying and pasting into a word processor. A reporter discovered the oversight and shared the material with NPR, which published TikTok's internal findings.²⁶³ Had the redaction worked as intended, or had TikTok not been in the geopolitical crosshairs, TikTok's own records showing that it had quantified the speed of addiction formation and considered its own safety tools as merely cosmetic might have remained sealed indefinitely. Notably, TikTok's appeal to the First Department challenges the very enforcement mechanism—state attorney general action—that was the only reason this concealed harm came to light. If TikTok prevails, the detection channel that exposed the harm will be narrowed for future cases of incognito consumer harm.²⁶⁴

The prescriptive lesson connects directly to this Article's framework, because *New York v. TikTok* simultaneously validates the *parens patriae* model and reveals its dependence on upstream detection. The New York Attorney General could sue because the investigation uncovered evidence that individual users structurally could not obtain. This is the complementarity between detection-first regulation and representative enforcement that this Article proposes: Regulatory tools generate information, and representative plaintiffs translate that information into accountability. For fully incognito harms, where no individual consumer might ever discover the injury, representative enforcement may be the only

262. *TikTok Inc. v. Garland*, 604 U.S. 56, 80 (2025).

263. See Bobby Allyn, Sylvia Goodman & Dara Kerr, *States Probed TikTok for Years. Here Are the Documents the App Tried to Keep Secret*, OPB (Oct. 11, 2024), <https://www.opb.org/article/2024/10/11/tiktok-knows-its-app-is-harming-kids-new-internal-documents-show/> [<https://perma.cc/6B72-5HUD>] (describing how the Kentucky Attorney General's complaint contained faulty redactions that could be bypassed by copying and pasting the text).

264. The irony is structural because TikTok's argument that individual users could bring claims themselves presupposes the very detection capacity that incognito harm is designed to defeat. If individual users cannot perceive the harm, the argument that they "could have" sued is circular: It treats the availability of a theoretical remedy as evidence that the remedy is adequate, when the point of incognito harm is that the theoretical remedy is unavailable in practice.

realistic litigation channel. The outcome of TikTok's appeal will test whether New York's courts recognize this structural necessity or allow the fire alarm objection, that individual users could have sued on their own, to foreclose the state's police patrol function.²⁶⁵

Finally, litigants can exploit the fraud-and-deception framing where it fits. Some incognito harms can be litigated when reframed as a misrepresentation or benefit-of-the-bargain deception, essentially arguing that "I would not have used a product had I known the truth." That framing can supply a more traditional injury narrative and sometimes fits within existing consumer protection doctrine. Courts already understand deception injuries better than "data handling" injuries, and litigants can exploit that doctrinal reality once concealment is punctured, without forcing every case into the same fraud-based model.

These litigation reforms aim to make concealment an *ex ante* liability risk rather than an *ex post* liability shield. Public-detection-first reforms can surface hidden harms, but private enforcement must translate discovery into viable claims through concealment-sensitive evidentiary rules, narrow early discovery, legislatively recognized injuries, and workable aggregation. Otherwise, incognito consumer harm will likely remain, in practice, a strategy of partial impunity.

D. Minor vs. Structural Reforms and Litigation vs. Regulation: A Synthesis

The reforms proposed in Sections B and C are not a menu from which policymakers should choose. They are components of a system that work best in combination. Start with the interaction between detection and

265. The appeal was pending before the First Department at the time of this Article's publication. The March 2026 jury verdicts in *P.F. v. Meta Platforms, Inc.*, No. 23SMCV03371 (Cal. Super. Ct. Mar. 25, 2026) (finding Meta and YouTube liable for negligent, defective platform design), and *State v. Meta Platforms, Inc.*, No. D-101-CV-2023-02838 (N.M. Dist. Ct. Mar. 24, 2026) (noting \$375 million in civil penalties for violations of New Mexico's Unfair Practices Act) suggest that courts and juries are increasingly willing to scrutinize social media design choices, though neither decision directly resolves the *parens patriae* or Section 230 questions presented in TikTok's First Department appeal. See, e.g., Bobby Allyn, *Jury Finds Meta and Google Negligent in Social Media Harms Trial*, NPR (Mar. 25, 2026, at 20:19 ET), <https://www.npr.org/2026/03/25/nx-s1-5746125/meta-youtube-social-media-trial-verdict> [<https://perma.cc/GL2G-XQHN>]; Press Release, N.M. Dep't of Just., New Mexico Department of Justice Wins Landmark Verdict Against Meta (Mar. 24, 2026), <https://nm DOJ.gov/press-release/new-mexico-department-of-justice-wins-landmark-verdict-against-meta/> [<https://perma.cc/3EDJ-2VJK>]; Beth Wang, *NY TikTok Addiction Case Hinges on State's Standing to Sue*, BLOOMBERG L. (Apr. 7, 2026, at 04:00 CT), <https://news.bloomberglaw.com/litigation/tiktok-banks-on-standing-question-to-nix-ny-addiction-case> [<https://perma.cc/2FL5-EQGE>] ("A ruling against TikTok on the standing issue in the New York case could 'signal to courts nationwide that state enforcement actions targeting addictive platform design are viable over objections that individual users should sue on their own,' said Yunsieg P. Kim . . .").

sanctions. The model of the expected cost of misconduct turns on the severity of punishment, the probability of getting caught,²⁶⁶ and, as Section II.C explained, timing—because delayed enforcement allows incognito harms to compound. The reforms proposed here therefore operate on all three margins: Regulatory tools raise the probability and speed of detection, while litigation reforms raise the severity of consequences once misconduct is exposed. High sanctions with near-zero detection produce a system that is strict on paper but permissive in practice, which is approximately the status quo. High detection with weak sanctions produces information without accountability: a regulatory apparatus that can see incognito harm but cannot make perpetrators pay for it. Treating detection and enforcement as complements rather than alternatives is essential.

The relationship between the two categories of reform is sequential in a given case but recursive across cases. Detection usually precedes litigation, as consumers cannot sue over what no one has discovered. But litigation can generate the facts, categories, and institutional lessons that shape tomorrow's detection duties. One exposed case can reveal which logs should have existed, which design choices suppressed awareness, and which audit questions to ask. Several of the litigation reforms in Section C become more defensible and easier to cabin once the regulatory reforms in Section B are in place. Limited pre-suit discovery, for instance, is less likely to become a fishing expedition if mandated audit trails create specific, checkable records. Constructive spoliation presumptions are easier to confine when whistleblower protections and auditability obligations help produce concrete evidence of efforts to defeat detection. Concealment-sensitive tolling is more administrable when regulators maintain portals that aggregate consumer verification requests, creating a record of when information was or was not available. In each case, upstream regulatory infrastructure reduces the downstream litigation risk that critics most fear: unbounded, costly, and indiscriminate private enforcement.

Such a risk is genuine, and the Article would be incomplete without acknowledging it. Detection-first reform can go wrong if implemented without discipline. A cautionary example involves Google's automated scanning of user content for child sexual abuse material. A father photographed his toddler's inflamed groin to send to a doctor for a remote consultation. Google's system flagged the photos as child sexual abuse material, the father's account was locked, and a police investigation was

266. See Garoupa, *supra* note 176, at 1765; A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45, 47 (2000) (arguing that one will commit a wrong "taking into account . . . the chance of his being caught and sanctioned"); *id.* at 47–55 (modeling offender behavior).

opened against him.²⁶⁷ The investigation found no wrongdoing, but the consequences were severe and the father's account was not restored. The episode illustrates what happens when detection operates without the safeguards this Article proposes: risk-based scope, data minimization, confidentiality controls, and independent human review before consequences attach. The goal of detection-first consumer protection is to build narrow, targeted, and accountable mechanisms that can verify compliance in domains where concealment is the primary enforcement obstacle, while preserving the privacy and autonomy that overbroad surveillance would destroy. The difference between responsible and irresponsible detection is design, and design is what this Article's proposals are about.²⁶⁸

The choice, then, is whether to build a coordinated system that raises both the probability of discovery and the cost of concealment, or to continue relying on a regime that waits for accidents to reveal what wrongdoers have engineered to remain unseen.

CONCLUSION

Existing consumer protection law subsidizes concealment. Even though no sound legislature sets out to reward concealment, the practical effect of the current system is indistinguishable from one that does. A firm that invests in making its misconduct invisible faces lower expected liability than one that commits the same misconduct openly, because the probability of detection collapses while sanctions remain tied to what is discovered. Doctrine reinforces the subsidy: Standing filters out injuries that leave no observable trace, pleading doctrine demands facts that concealment withholds, and class certification fractures precisely where concealment succeeds. The result is a system in which the most successful wrongdoers are the least likely to face consequences because they are the most effective at rendering themselves invisible.

This Article has argued that the subsidy can be reversed. Detection-first regulatory tools, including verification rights structured as tiered petitions,

267. Johana Bhuiyan, *Google Refuses to Reinstate Man's Account After He Took Medical Images of Son's Groin*, GUARDIAN (Aug. 22, 2022, at 19:32 ET), <https://www.theguardian.com/technology/2022/aug/22/google-csam-account-blocked> [https://perma.cc/EU3E-CS9E]; see also Kashmir Hill, *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.*, N.Y. TIMES (June 21, 2023), <https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html> [https://perma.cc/9C4P-PJRQ].

268. See *supra* Section III.B.2 (proposing risk-based telemetry with data minimization, confidentiality controls, and limited-purpose access); *supra* note 215 and accompanying text (discussing hashing, counters, and event metadata as privacy-preserving logging techniques).

auditability by design, and whistleblower and intermediary reporting incentives, can raise the probability that hidden practices are discovered. Litigation reforms, including constructive spoliation, narrow early discovery, legislatively recognized injuries, and representative enforcement, can ensure that discovery translates into accountability. Together, these reforms treat concealment as an aggravating factor rather than a liability shield, making invisibility costly rather than profitable.

The stakes will only rise in the years to come. As AI intensifies firms' appetite for granular consumer data and as commerce shifts toward opaque intermediaries and disposable sellers, the payoff to undetectable extraction increases. A legal system built for visible injuries cannot remain credible in such a world. It must stop treating invisibility as a practical inconvenience and start treating it as the central wrong. The objective is not to invent liability for every technological discomfort, but to prevent modern injuries from disappearing merely because courts can recognize them only when they pretend to be old ones.